TeleWell

TW-EA2000 ADSL modeemi/palomuuri/reititin+ WLAN tukiasema (802.11 b+g)

Ohjekirja

CE

Tarkemmat asetusohjeet palomuurille, DynDNS:lle, porttisuotimille ja muille erikoisominaisuuksille ovat vain englanninkielisessä ohjekirjassa.

Laite toimii oletusasetuksilla Sonera, Elisa, Saunalahti, DNA, Baana, MTV3, PHP, Kymppi, VLP jne. ADSL-liittymissä.

Perustila:

* Laite hakee IP-osoitteen itselleen ja jakaa sen DHCP + NAT toiminnolla sisäverkkoon
* Vain NAT-palomuuri on päällä oletuksena
* Palomuuri pitää laittaa päälle erikseen kuten myös hyökkäysten tunnistus ja estot. Muista määritellä porttisuotimet.

*** Palomuurin Medium tasolla toimivat www-selaus, sähköpostit (pop) ja pankkipalvelut. Palomuurin LOW-tasolla toimii myös MSN- yms. sovellukset. High-tasolla kaikki portit pitää määritellä itse.**

Myyntipaketin sisältö

- TELEWELL TW-EA2000 ADSL modeemi
- CD-ROM levy, jossa ohjekirjan kopio
- RJ-11 puhelinjohto ja suomalainen puhelinpistoke
- Ethernet- (CAT-5 LAN) kaapeli (suora)
- Konsoli- (PS2-RS232) kaapeli
- AC-DC virtalähde (12VDC, 1A)
- Ohjekirja

Varoitukset

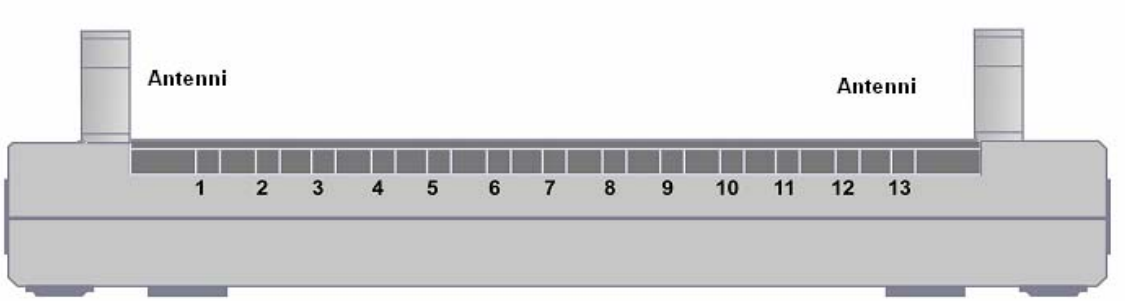
Laitetta saa käyttää vain normaaleissa asuinhuoneen lämpö- ja kosteusolosuhteissa. Käytä vain laitteen mukana tullutta verkkovirta-muuntajaa.

Laitteen avaaminen ei ole sallittua ilman Easytel Oy:n lupaa. Jos laite on avattu ilman lupaa, niin takuu lakkaa välittömästi.

Huomautus

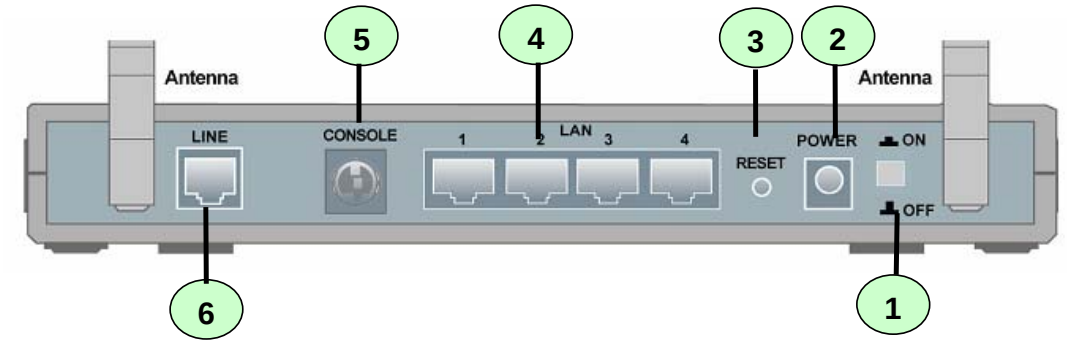
Pidä laitetta mahdollisimman pölyttömässä paikassa.
Älä aseta laitetta muiden lämpöä tuottavien laitteiden päälle eikä monitorien tai GSM-puhelinten viereen.

Etupanelin merkkivalot



Merkkivalo		Toiminto
1	PWR	Merkkivalo palaa, kun virta on päällä.
2	SYS	Merkkivalo palaa, kun järjestelmä on toimintavalmis.
3	LAN port 1	Merkkivalo palaa, kun verkkokaapeli on kytketty. Väri on vihreä, kun nopeus 100 Mbps. Oranssi väri tarkoittaa 10 Mbps nopeutta. Merkkivalo vilkkuu, kun tietoa siirretään.
4	LAN port 2	Merkkivalo palaa, kun verkkokaapeli on kytketty. Väri on vihreä, kun nopeus 100 Mbps. Oranssi väri tarkoittaa 10 Mbps nopeutta. Merkkivalo vilkkuu, kun tietoa siirretään.
5	LAN port 3	Merkkivalo palaa, kun verkkokaapeli on kytketty. Väri on vihreä, kun nopeus 100 Mbps. Oranssi väri tarkoittaa 10 Mbps nopeutta. Merkkivalo vilkkuu, kun tietoa siirretään.
6	LAN port 4	Merkkivalo palaa, kun verkkokaapeli on kytketty. Väri on vihreä, kun nopeus 100 Mbps. Oranssi väri tarkoittaa 10 Mbps nopeutta. Merkkivalo vilkkuu, kun tietoa siirretään.
7	WLAN	Merkkivalo palaa, kun WLAN tukiasema on toimintavalmis. Merkkivalo vilkkuu, kun tietoa siirretään.
10	MAIL	Merkkivalo vilkkuu, kun sähköpostia on saapunut. Toiminta pitää laittaa erikseen päälle.
11	PPP	Merkkivalo palaa, kun yhteysprotokolla on PPPoA / PPPoE.
13	ADSL	Merkkivalo palaa, kun yhteys on kytketty operaattorin ADSL-keskukselle. Merkkivalo vilkkuu, kun modeemi hakee keskuksen modeemia tai operaattorin kytkentä on tekemättä tai puhelinlinjassa on vikaa.

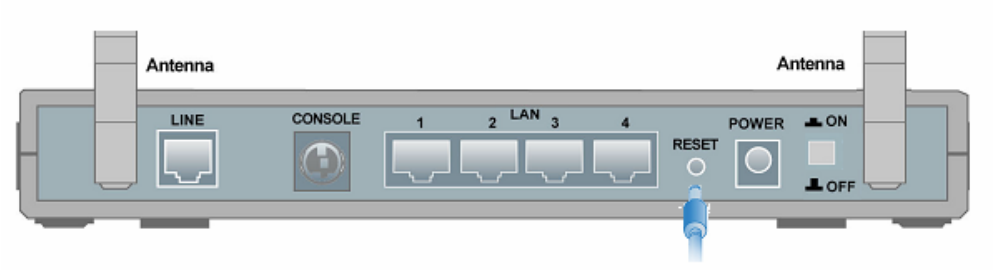
Takapanelin merkkivalot



Toiminto		Tarkoitus
1	**Virtakytkin**	Power ON/OFF eli virta päälle/pois päältä
2	**PWR**	Merkkivalo palaa, kun sähkövirta on päällä.
3	**RESET**	Reset-näppäimen toiminnot, kun näppäin pidetään painettuna pohjaan: **0-3 sekunttia:** käynnistää modeemin uudelleen **6 sekunttia tai yli:** palauttaa tehdasasetukset
4	**LAN** **1X — 4X** **(RJ-45 connector)**	Kytketään UTP Ethernet-kaapeli (Cat-5 tai Cat-5e) johonkin 4 portista. Kaapelin toinen pää liitetään tietokoneen verkkokorttiin.
5	**CONSOLE**	Kytketään tarvittaessa PS2/RS-232 kaapeli tietokoneen ja laitteen välille erikoisohjelmointia varten, esimerkiksi ”flash-muistin” korjaus”
6	**LINE**	Laite kytketään yleiseen puhelinverkkoon ADSL-yhteyttä varten.

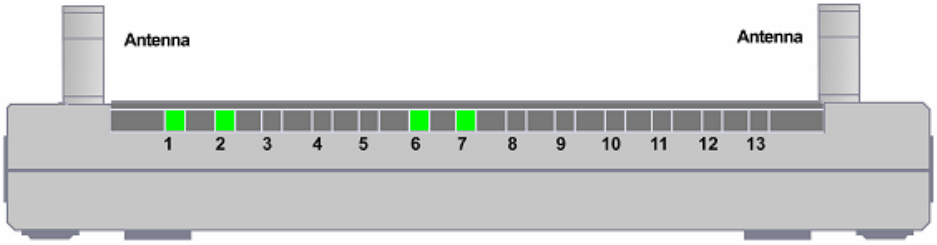
ADSL modeemin käyttöönotto

1. Kytke puhelinjohto LINE-liittimeen: RJ-11 puhelinjohto
2. Kytke tietokoneet LAN 1-4 portteihin: Cat5 ethernet-kaapeli (suora)
3. Kytke laitteen virta päälle: power on



Tarkista seuraavat seikat, kun laite on käynnistynyt kokonaan:

4. PWR-merkkivalo on päällä (1)
5. SYS-merkkivalo on päällä (2)
6. WLAN-merkkivalo on päällä (7)
7. ADSL-merkkivalo on päällä (13)
8. LAN-merkkivalo palaa siinä portissa, mihin ethernet-kaapeli on kytketty (6)



Adsl-merkkivalo valo vilkkuu, kunnes laite on löytänyt adsl-keskuksen. Mikäli adsl-valo ei jää palamaan, niin tarkista puhelinkytkennät. **Jokainen analoginen puhelinlaite pitää eriyttää ADSL-modeemin signaaleista häiriösuotimella.**

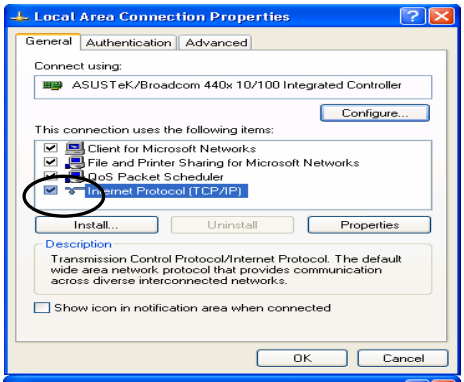
ADSL modeemi kytketään puhelinverkkoon aina ilman häiriösuodatinta.

Windows-tietokoneen asetukset (TCP/IP)

1. **Windows käyttöjärjestelmässä**

   Siirry kohtaan ohjainpaneeli/ verkkoasetukset

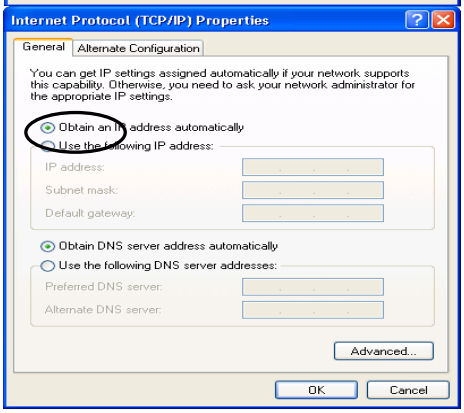
2. Valitse verkkoyhteydet ja verkkokortin ominaisuudet
3. Valitse TCP/IP ja sen ominaisuudet



4. **Tee asetus mallikuvan mukaiseksi eli IP-osoite haetaan automaattisesti.**

   Valinta kohta vaihtelee jonkin verran riippuen siitä, mikä Windows-versio on kyseessä

   Mac OS-versioissa asetus on kohdassa Omenavalikko / Laajennukset / TCP/IP, jossa valitaan DHCP päälle ja oikea verkkosovitin

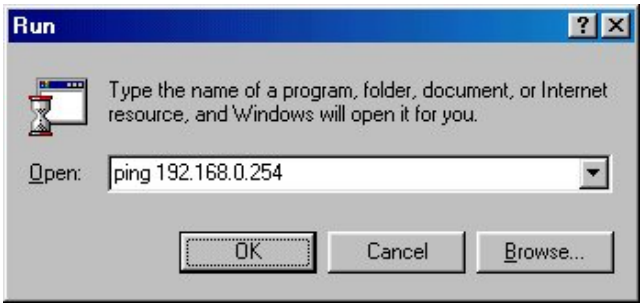

Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

ADSL-modeemin perusasetukset

Laitteen asetusten muutokset tehdään Internet-selaimella:
IE5 tai uudempi, Netscape 4.6 tai uudempi tai Opera 7

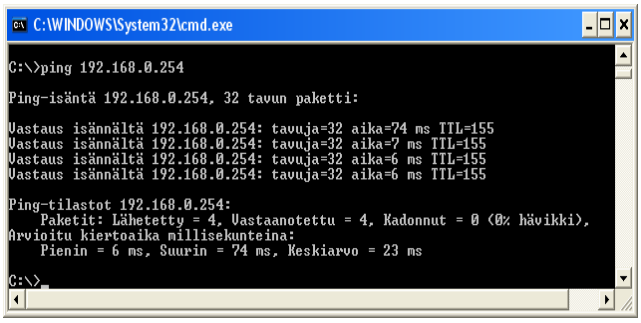
Oman verkon toimivuuden tarkistus

Suorita-toiminto
Käynnistä / Suorita
ping 192.168.0.254
ja valitse ok.



Modeemin pitää vastata PING-komentoon.

Jos vastausta ei tule, niin tarkista, että verkkokortin IP-osoitteen haku on automaattisella asetuksella ja verkkokaapeli on kytketty oikein tietokoneen ja modeemin välille.


C:\WINDOWS\System32\cmd.exe
C:\>ping 192.168.0.254
Ping-isäntä 192.168.0.254, 32 tavun paketti:
Vastaus isännältä 192.168.0.254: tavuja=32 aika=74 ms TTL=155
Vastaus isännältä 192.168.0.254: tavuja=32 aika=7 ms TTL=155
Vastaus isännältä 192.168.0.254: tavuja=32 aika=6 ms TTL=155
Vastaus isännältä 192.168.0.254: tavuja=32 aika=6 ms TTL=155
Ping-tilastot 192.168.0.254:
Paketit: Lähetetty = 4, Vastaanotettu = 4, Kadonnut = 0 (0% hävikki),
Arvioitu kiertoaika millisekunteina:
Pienin = 6 ms, Suurin = 74 ms, Keskiarvo = 23 ms
C:\>

Yhteys laitteen hallintaohjelmistoon

Avaa Internet-selain ja anna osoitteeksi
http://192.168.0.254
ja painan **Enter**-näppäintä

WWW-selaimessa ei saa olla ”proxy”- eli välityspalvelinasetus päällä. Muut palomuuriohjelmat voivat häiritä laitteen hallintaa.

Oletustunnukset: **User Name ja Password “admin” ja ”admin”.** Valitse **OK.**

Salasanojen palautus, jos niitä muutettu: katso laitteen reset -näppäimen toiminta

ADSL modeemin oletusasetukset

- **WWW-hallinta:**
  - User name: admin
  - Password: admin

- **LAN liite:**
  - IP-Address: 192.168.0.254
  - Subnet Mask: 255.255.255.0

- **ADSL-operaattori asetukset:**
  - RFC 1483 tila ja LLC sillattu kehysrakenne

- **DHCP palvelin:**
  - DHCP on päällä.
  - IP-alue alkaen: 192.168.0.100
  - IP-osoitteiden oletuksena jaettava määrä: 100

- **WLAN:**
  - Tukiaseman nimi (ESSID): WLAN-AP
  - Kanavan numero (Channel ID): Channel 6
  - Tukiaseman piilotus (Hide_SSID): False = pois päältä

- **VPI / VCI Settings:**
  - 0 / 33
  - 0 / 100 tai tunnnistaa automaattisesti useita operaattoreita
  - 14 / 24

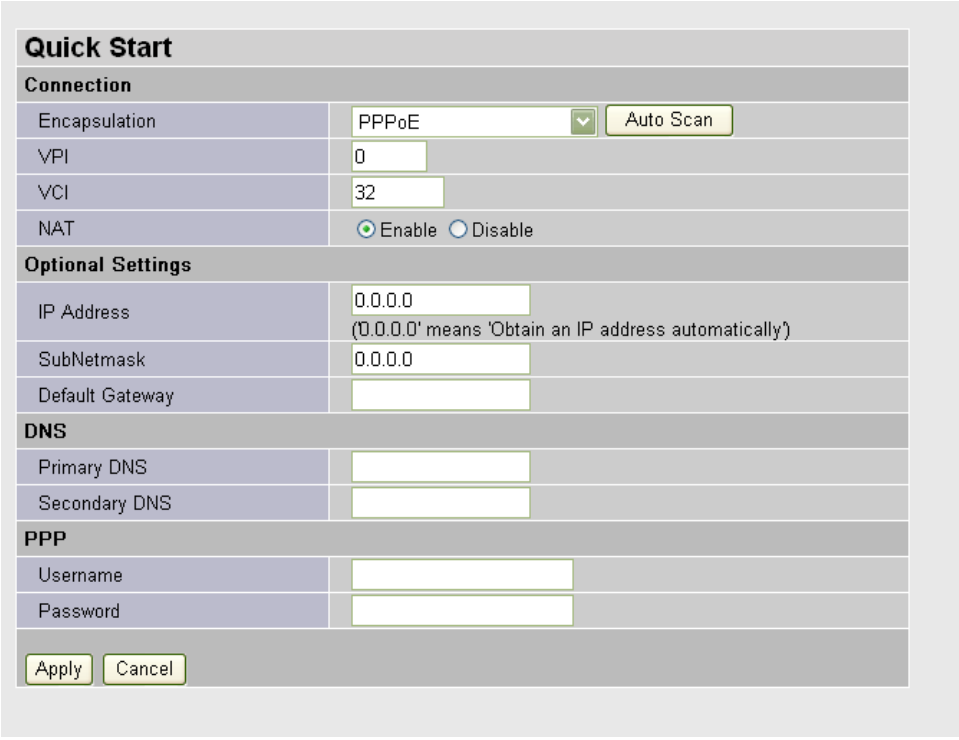
  Toimii suoraan Soneran, Elisan, Baanan, Dna:n, Saunalahden, VLP:n, PHP:n, Kympin jne. liittymissä. Jos käytät PPPoE- tai PPPoA-operaattoreita kuten PPO, OPOY, Saunalahti ADSL+ tai muita vastaavia liityntöjä, niin katso ohje seuraavalta sivulta **!**

PPPoA ja PPPoE protokollat

Saunalahti ADSL+, Oulun Puhelin, Pohjanmaan puhelin
Kajaanin Puhelin Liittymät

Poista oletusprofiilit kohdasta asetukset / WAN / ISP
Luo pikakäynnistys-toiminnolla uusi oma asetus.
Käytä AUTO SCAN -toimintoa, normaalisti PPPoA.

Muista tallentaa löydetty asetus → apply / tallenna
+ ”tallennus flash-muistiin” -toiminto



TW-EA2000

802.11g ADSL VPN Firewall Router

User's Manual

Table of Contents

CHAPTER 1: INTRODUCTION.....3

INTRODUCTION TO YOUR TW-EA2000 ROUTER.....3
SUPPORT.....3
FEATURES.....3
TW-EA2000 ADSL ROUTER APPLICATION.....6

CHAPTER 2: INSTALLING THE ROUTER ...7

IMPORTANT NOTE FOR USING THE TW-EA2000 ADSL ROUTER.....7
PACKAGE CONTENTS.....7
THE FRONT LEDS.....8
THE REAR PORTS.....9
CABLING.....10

CHAPTER 3: BASIC INSTALLATION 11

CONNECTING YOUR ROUTER.....12
Configuring PCs in Windows Windows XP.....13
Windows 2000.....14
Windows 98 / ME.....15
Windows NT4.0.....16
FACTORY DEFAULT SETTINGS.....17
Username and Password.....17
LAN and WAN Port Addresses.....18
INFORMATION FROM YOUR ISP.....19
CONFIGURING WITH YOUR WEB BROWSER.....20

CHAPTER 4: CONFIGURATION 21

STATUS.....22
ARP Table.....22
Routing Table.....23
DHCP Table.....24
PPTP Status.....25
IPSec Status.....26
L2TP Status.....26

Email Status *27*
Event Log *27*
Error Logging *28*
UPnP Portmap *28*
QUICK START 29
CONFIGURATION 31
LAN (Local Area Network) *31*
WAN (Wide Area Network) *38*
System *49*
Firewall and Access Control *54*
VPN (Virtual Private Networks) *68*
QoS (Quality of Service) *91*
Virtual Server ("Port Forwarding") *94*
Advanced *97*
SAVE CONFIGURATION TO FLASH 104
LOGOUT 105

CHAPTER 5: TROUBLESHOOTING 106

PROBLEMS STARTING UP THE ROUTER 106
PROBLEMS WITH THE WAN INTERFACE 106
PROBLEMS WITH THE LAN INTERFACE 107

APPENDIX A: PRODUCT SUPPORT AND CONTACT INFORMATION 108

Chapter 1: Introduction

Introduction to your TW-EA2000 Router

Welcome to the TeleWell TW-EA2000 Wireless Router. Your TeleWell router is an "all-in-one" unit, combining an ADSL modem, ADSL router and Ethernet network switch, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection. With features such as an ADSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

Support

This manual will guide you through configuring your router using its web browser interface – all you need to setup and manage your new router is a web browser! If you have any questions or problems that you can't find the answer for in this manual, please visit the TeleWell website at http://www.easytel.fi/

Features

- **ADSL Multi-Mode Standard**
  Supports downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G992.2)). The Annex A and B are supported in different H/W platforms.
- **Wireless Ethernet 802.11g**
  With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP and WPA for securing your wireless networks. The TW-EA2000 has included the first solution for turbo charging 802.11g systems called PRISM Nitro. It provides up to 50% greater .

  throughput performance in homogenous 802.11g networks and enhanced protection mechanisms to significantly increase mixed-mode network performance.

- **Fast Ethernet Switch**
  A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or cross-over cable can be used directly for auto detection.

- **Multi-Protocol to Establish A Connection**
  Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) and PPTP-to-PPPoA relaying to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.
- **Quick Installation Wizard**
  Supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.
- **Universal Plug and Play (UPnP) and UPnP NAT Traversal**
  This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.
- **Network Address Translation (NAT)**
  Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.
- **Firewall**
  Supports SOHO firewall with NAT technology, automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall functions will always be implemented through updated firmware releases.
- **Domain Name System (DNS) relay**
  Provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.
- **Dynamic Domain Name System (DDNS)**
  The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.
- **Virtual Private Network (VPN)**
  Allows user to make a tunnel with a remote site directly to secure the data transmission among the connection. User can use embedded PPTP client/server, IKE and IPSec which are supported by this router to make a VPN connection or users can run the PPTP client in PC and the router already provides IPSec and PPTP pass through function to establish a VPN connection if the user likes to run the PPTP client in his local computer.
- **Virtual Server ("port forwarding")**
  Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the

specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

- **Rich Packet Filtering**
  Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.
- **Dynamic Host Configuration Protocol (DHCP) client and server**
  In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **Static and RIP1/2 Routing**
  Supports an easy static routing table or RIP1/2 routing protocol to support routing capability.
- **Simple Network Management Protocol (SNMP)**
  It is an easy way to remotely manage the router via SNMP.
- **Web based GUI**
  Supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.
- **Firmware Upgradeable**
  Device can be upgraded to the latest firmware through the WEB based GUI.
- **Rich management interfaces**
  Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

TW-EA2000 ADSL Router Application

Figure 1.1 Application Diagram

Thank you for your purchase, and welcome to the world of broadband Internet!

Chapter 2:
Installing the Router

Important note for using the TW-EA2000 ADSL Router

Warning

- ✓ Do not use the TW-EA2000 in high humidity or high temperatures.
- ✓ Do not use the same power source for the TW-EA2000 as other equipment.
- ✓ Do not open or repair the case yourself. If the TW-EA2000 is too hot, turn off the power immediately and have it repaired at a qualified service center.

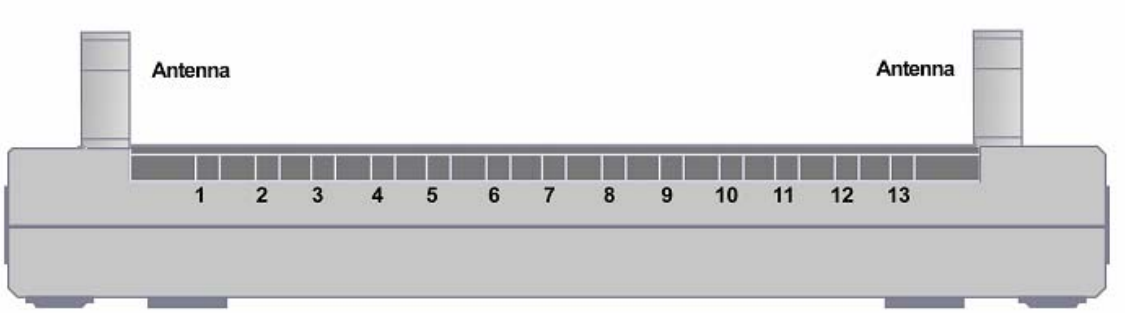
Attention

- ✓ Place the TW-EA2000 on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Package Contents

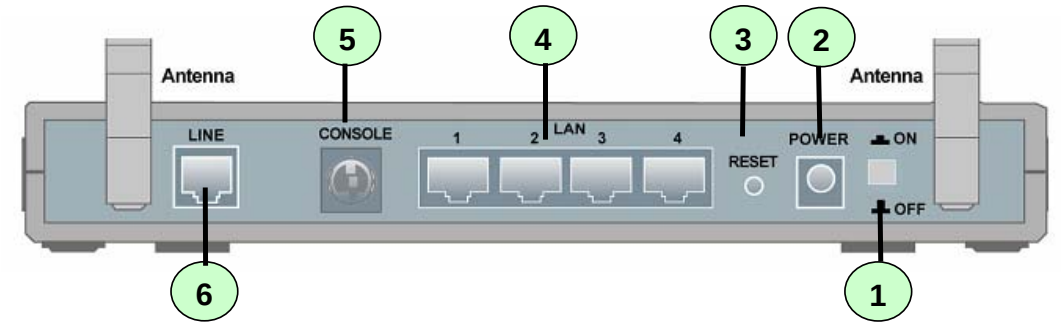
- TW-EA2000 ADSL VPN Firewall Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5 LAN) Cable
- Console (PS2-RS232) Cable
- AC-DC power adapter (12VDC, 1A)
- Quick Start Guide

The Front LEDs



LED		Meaning
1	PWR	Lit when power is ON.
2	SYS	Lit when the system is ready.
3	LAN port 1	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps Blinking when data is transmitted/received.
4	LAN port 2	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps Blinking when data is transmitted/received.
5	LAN port 3	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps Blinking when data is transmitted/received.
6	LAN port 4	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps Blinking when data is transmitted/received.
7	WLAN	Lit green when the wireless connection is established. Flashes when sending/receiving data.
10	MAIL	Flash when there is Email in your configured Email account.
11	PPP	Lit when there is a PPPoA / PPPoE connection.
13	ADSL	Lit when successfully connected to an ADSL DSLAM (“linesync”).

The Rear Ports



Port		Meaning
1	**Power Switch**	Power ON/OFF switch
2	**PWR**	Connect the supplied power adapter to this jack.
3	**RESET**	After the device is powered on, press it to reset the device or restore to factory default settings. **0-3 seconds**: reset the device **6 seconds above**: restore to factory default settings (this is used when you cannot login to the router. **E.g. forgot the password**)
4	**LAN** **1X — 4X** **(RJ-45 connector)**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
5	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
6	**LINE**	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/telephone network.

Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your TeleWell router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Chapter 3:
Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me, etc. The product provides a very easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.0.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.0.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

Any TCP/IP capable workstation can be used to communicate with or through the TW-EA2000. To configure other types of workstations, please consult the manufacturer's documentation.

Connecting your router

1. Connect the Router to a LAN (Local Area Network) and the ADSL/telephone network.
2. Power on the device.
3. Make sure the PWR, SYS and WLAN LEDs are lit steadily and that the relevant LAN LED is lit.

Configuring PCs in Windows

Windows XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.

2. Double-click **Local Area Connection**. **(See Figure 3.1)**

3. In the **LAN Area Connection Status** window, click **Properties**. (**See Figure 3.2)**

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (**See Figure 3.3)**

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (**See Figure 3.4**)

6. Click **OK** to finish the configuration.

Figure 3.1: LAN Area Connection

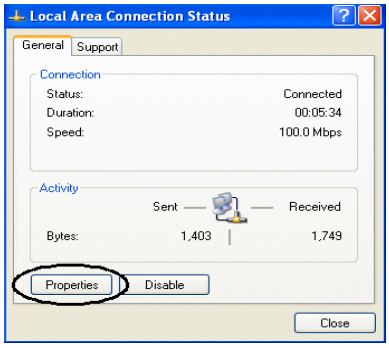


Figure 3.2: LAN Connection Status

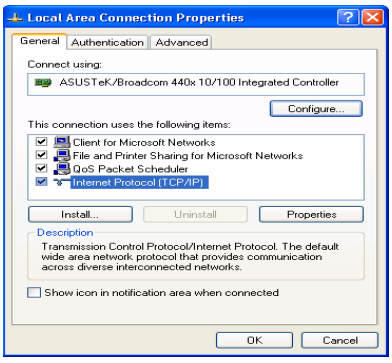


Figure 3.3: TCP / IP

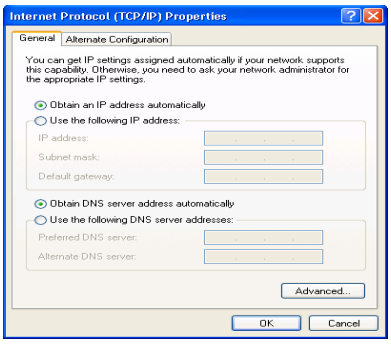

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3.4: IP Address & DNS Configuration

Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network and Dial-up Connections**.

2. Double-click **Local Area ("LAN") Connection**. **(See Figure 3.5)**

3. In the **LAN Area Connection Status** window, click **Properties**. **(See Figure 3.6)**

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. **(See Figure 3.7)**

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. **(See Figure 3.8)**

6. Click **OK** to finish the configuration.

Figure 3.5: LAN Area Connection

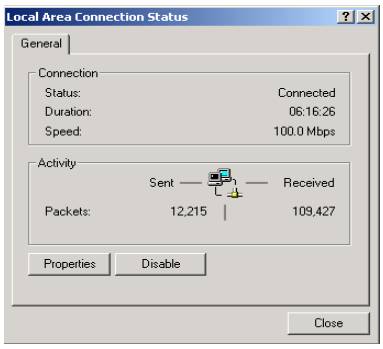


Figure 3.6: LAN Connection Status

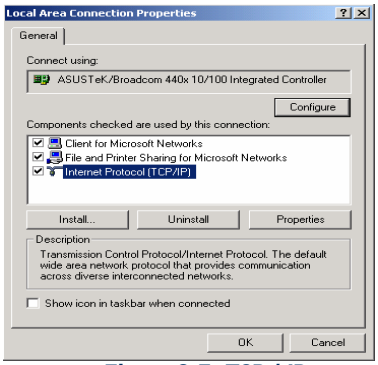


Figure 3.7: TCP / IP

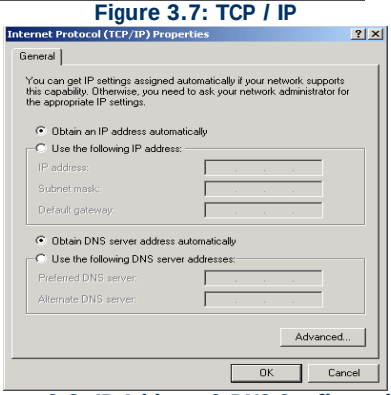

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3.8: IP Address & DNS Configuration

Windows 98 / ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Configuration** tab.

2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC. (**See Figure 3.9)**

3. Click **Properties**.

4. Select the **IP Address** tab. In this page, click the Obtain an IP address automatically radio button. (**See Figure 3.10)**

5. Then select the **DNS Configuration** tab. **(See Figure 3.11)**

6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

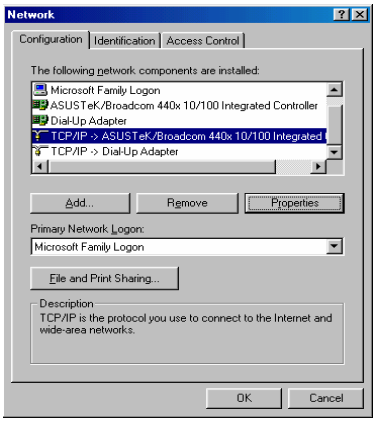


Figure 3.9: TCP / IP

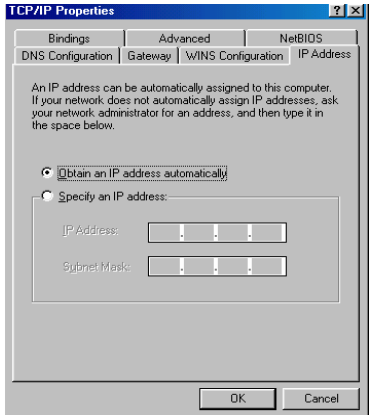

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 3.10: IP Address

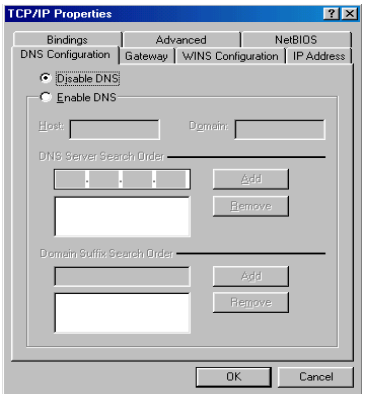


Figure 3.11: DNS Configuration

Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**. (**See Figure 3.12)**

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**. (**See Figure 3.13)**

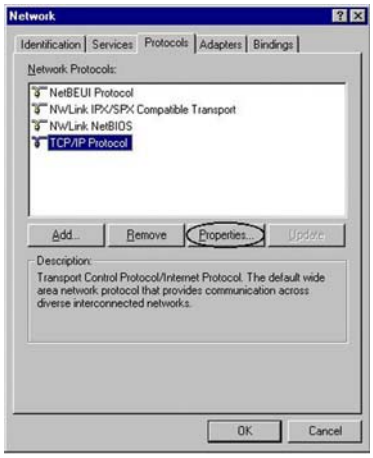


Figure 3.12: TCP / IP

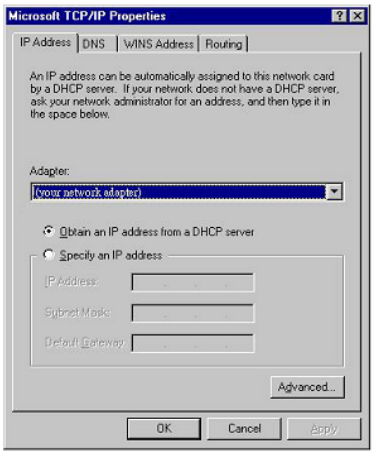

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[your network adapter]
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 3.13: IP Address

Factory Default Settings

Before configuring your, you need to know the following default settings.

- **Web Interface:**
  - Username: admin
  - Password: admin

- **LAN Device IP Settings:**
  - IP Address: 192.168.0.254
  - Subnet Mask: 255.255.255.0

- **ISP setting in WAN site:**
  - RFC 1483 Routed Mode with LLC Bridged Encapsulation

- **DHCP server:**
  - DHCP server is enabled.
  - Start IP Address: 192.168.0.100
  - IP pool counts: 100

- **DHCP server:**
  - ESSID: WLAN-AP
  - Channel ID: Channel 6
  - Hide_SSID: False

- **VPI / VCI Settings:**
  - 0 / 33
  - 0 / 100
  - 14 / 24

Username and Password

The default username and password are **"admin"** and **"admin"** respectively.

Attention

If you ever forget the password to log in, you may press the RESET button to restore the factory default settings.

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.0.254	The RFC 1483 Routed Mode function is *enabled* to automatically get the WAN port configuration from the ISP, but you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.0.100 through 192.168.0.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IPoA, or PPTP-to-PPPoA Relaying.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
IPoA	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **192.168.0.254**, and click **"Go"**, a user name and password window prompt will appear. **The default username and password are "admin" and "admin". (See Figure 3.14)**

Figure 3.14: User namd & Password Prompt Widonw

Congratulation! You are now successfully logon to the TW-EA2000 ADSL Router!

Chapter 4: Configuration

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status** (ARP Table, Routing Table, DHCP Table, PPTP Status, IPSec Status,L2TP Status, Email Status, Event Log, Error Log and UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, VPN, QoS, Virtual Server & Advanced)
- **Save Config to FLASH**
- **Language** (provides user interface in English and Finnish languages).

Please see the relevant sections of this manual for detailed instructions on how to configure your TeleWell router.

Status

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

ARP Table

IP <> MAC List

IP Address	MAC Address	Interface	Static
192.168.1.225	00:e0:18:e5:14:88	iplan	no

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

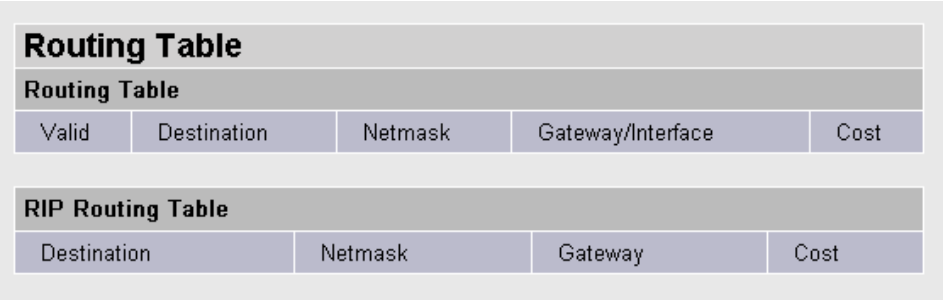
MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

- "**no**" for dynamically-generated ARP table entries
- "**yes**" for static ARP table entries added by the user

Routing Table



Routing Table:

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table:

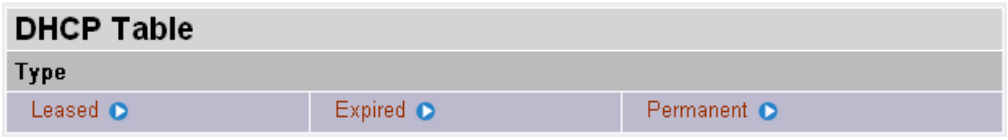
Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway: The IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

DHCP Table



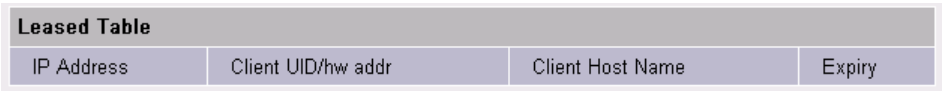
Leased: The DHCP assigned IP addresses information.

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table



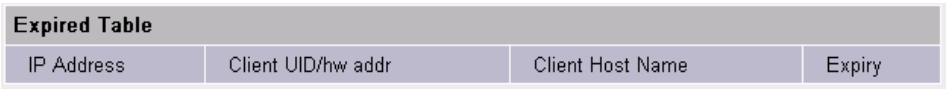
IP Address: The IP address that assigned to client.

Client UID/hw addr: The MAC address of client.

Client Host Name: The Host Name (Computer Name) of client.

Expiry: The current lease time of client.

Expired Table



Please refer the **Leased Table**.

Permanent Table

Name: The name you assigned to the Permanent configuration.

IP Address: The fixed IP address for the specify client.

MAC Address: The MAC Address that you want to assign the fixed IP address

Maximum Lease Time: The maximum lease time interval you allow to clients

PPTP Status

This shows details of your configured PPTP VPN Connections.

PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular PPTP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

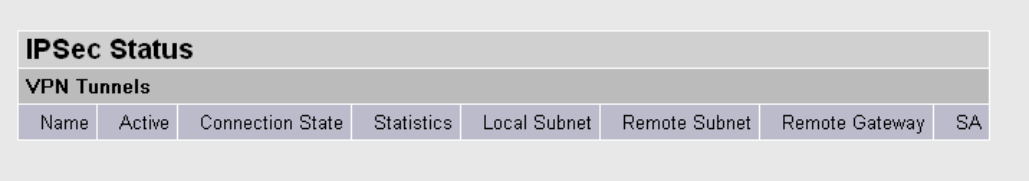
Tunnel Connected: Whether the VPN SessionTunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

IPSec Status

This shows details of your configured IPSec VPN Connections.

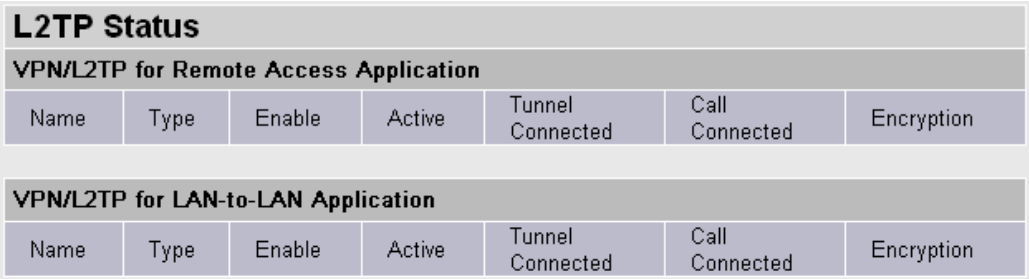


IPSec Status							
VPN Tunnels							
Name	Active	Connection State	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA

Name: The name you assigned to the particular VPN entry.
Active: Whether the VPN Connection is currently Active.
Connection State: Whether the VPN is Connected or Disconnected.
Statistics: Statistics for this VPN Connection.
Local Subnet: The local IP Address or Subnet used.
Remote Subnet: The Subnet of the remote site.
Remote Gateway: The Remote Gateway IP address.
SA: The Security Association for this VPN entry.

L2TP Status

This shows details of your configured L2TP VPN Connections.



L2TP Status						
VPN/L2TP for Remote Access Application						
Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption
VPN/L2TP for LAN-to-LAN Application						
Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

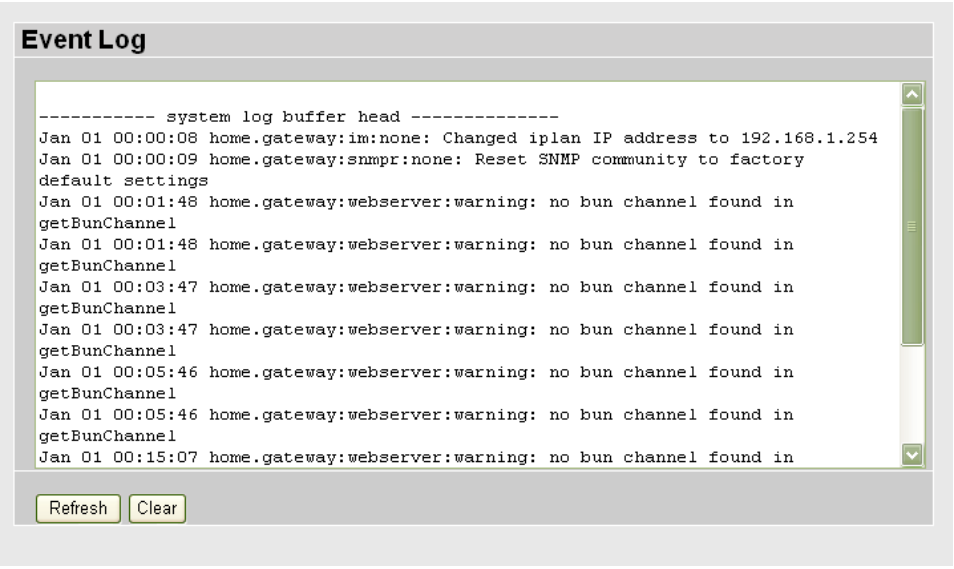
Name: The name you assigned to the particular L2TP connection in your VPN configuration.
Type: The type of connection (dial-in/dial-out).
Enable: Whether the connection is currently enabled.
Active: Whether the connection is currently active.
Tunnel Connected: Whether the VPN Tunnel is currently connected.
Call Connected: If the Call for this VPN entry is currently connected.
Encryption: The encryption type used for this VPN connection.

Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.

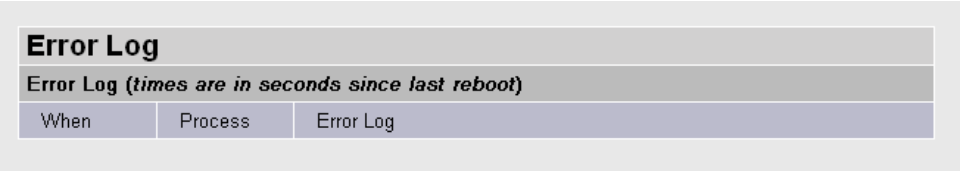
Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's ADSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.


Event Log
---------- system log buffer head --------------
Jan 01 00:00:08 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 01 00:00:09 home.gateway:snmpr:none: Reset SNMP community to factory default settings
Jan 01 00:01:48 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:01:48 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:03:47 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:03:47 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:05:46 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:05:46 home.gateway:webserver:warning: no bun channel found in getBunChannel
Jan 01 00:15:07 home.gateway:webserver:warning: no bun channel found in
Refresh
Clear

Error Logging

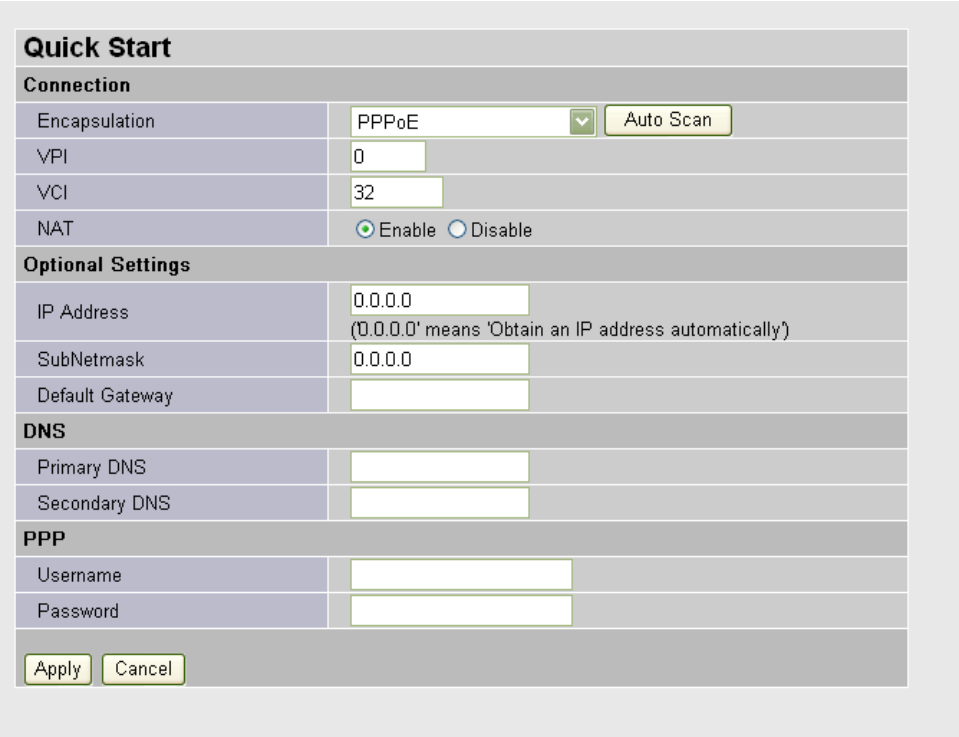
Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.



UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the **Advanced** section of this manual for more details on UPnP and the router's UPnP configuration options.

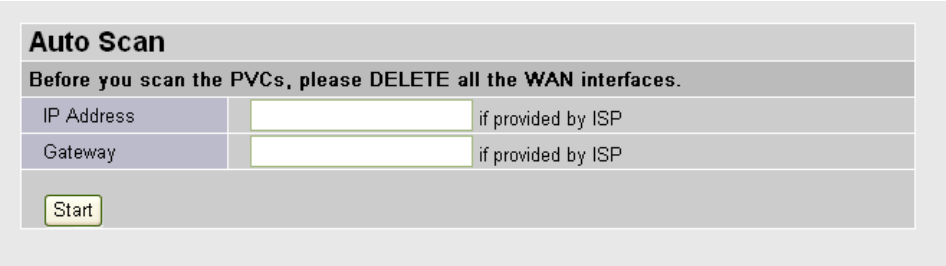
Quick Start



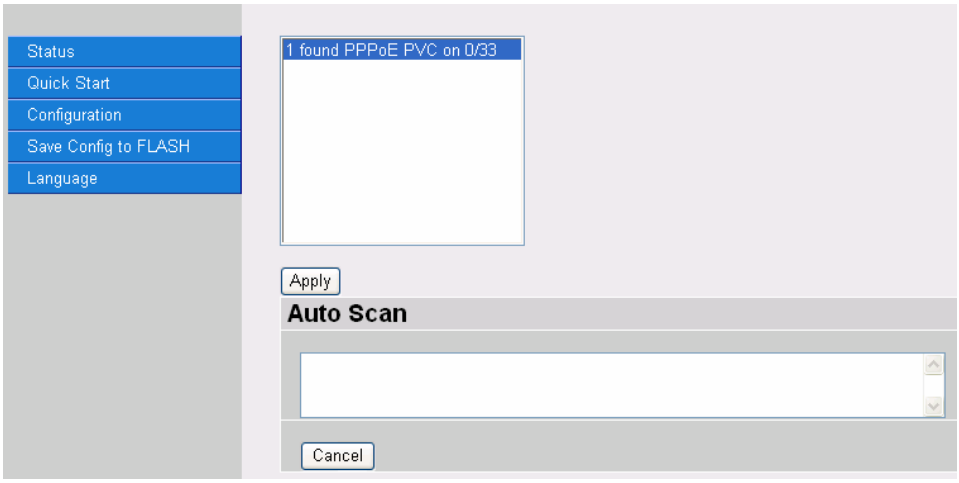
For detailed instructions on configuring your WAN settings, please see the **WAN** section of this manual.

Usually, the only details you will need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password and then encapsulation type.

Your ISP will be able to supply all the details you need, alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to attempt to determine the Encapsulation types offered by your ISP.



Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful you will then be presented with a list of supported options:



Select the desired option from the list and click **Apply** to return to the Quick Start interface to continue configuring your ISP connection. Please note that the contents of this list will vary, depending on what is supported by your ISP.

Configuration

When you click this item, you get following sub-items to configure the ADSL router.

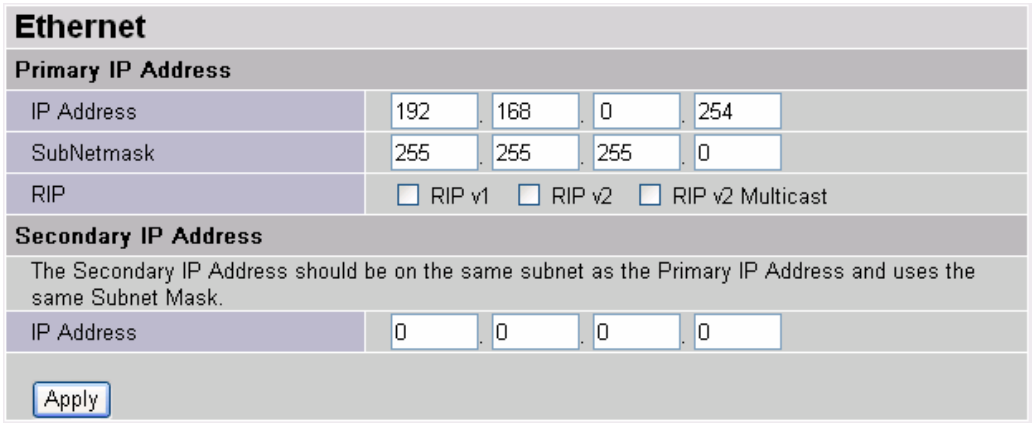
LAN, WAN, System, Firewall, VPN, QoS, Virtual Server and **Advanced**

These functions are described below in the following sections.

LAN (Local Area Network)

There are four items within the LAN section: **Ethernet, Wireless, Wireless Security, Port Setting** and **DHCP Server**.

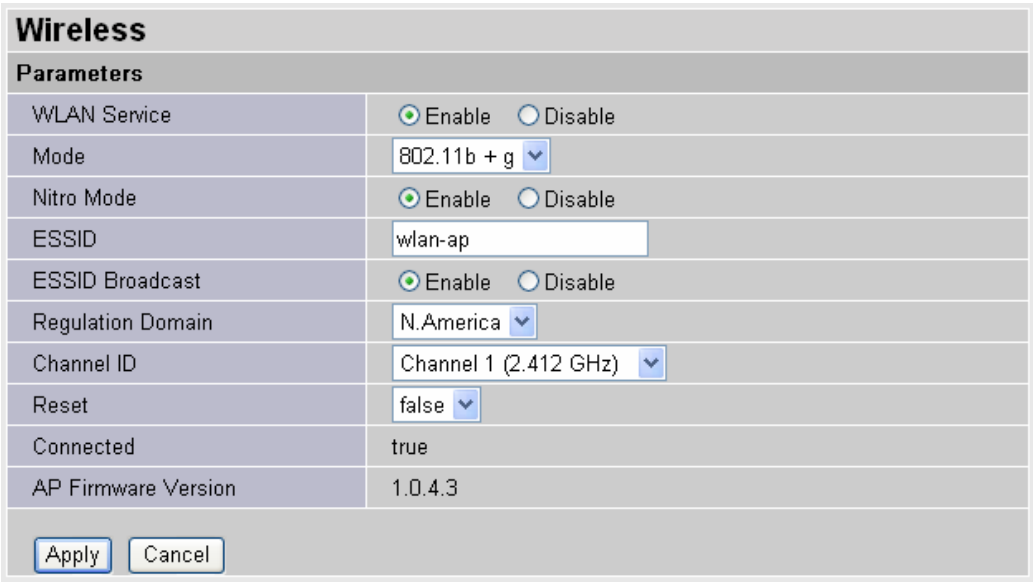
Ethernet


Ethernet
Primary IP Address
IP Address
192 . 168 . 0 . 254
SubNetmask
255 . 255 . 255 . 0
RIP
RIP v1 RIP v2 RIP v2 Multicast
Secondary IP Address
The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask.
IP Address
0 . 0 . 0 . 0
Apply

The router supports two Ethernet IP addresses in the LAN, and two different LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN, so there is no need to configure a Secondary IP address. The default IP address for the router is 192.168.0.254.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

Wireless



WLAN Service: Default setting is set to Enable.

Mode: 802.11b + g (Mixed mode), 802.11b and 802.11g. The factory default is 802.11b + g.

Nitro Mode: Default is enabled for increasing performance in mixed 802.11b and 802.11g wireless networks.

ESSID: Enter the unique ID given to the Access Point (AP), which is already built-in to the router's wireless interface. To connect to this device, your wireless clients must have the same ESSID as the device.

ESSID Broadcast:

⊙ **Disable:** Any client that using the "any" setting cannot discover the Access Point (AP) in question.

⊙ **Enable:** Any client that using the "any" setting can discover the Access Point (AP) in question.

Regulation Domain: There are five Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Reset: Reset the Access Point (AP), which is already built-in to the router's wireless interface.

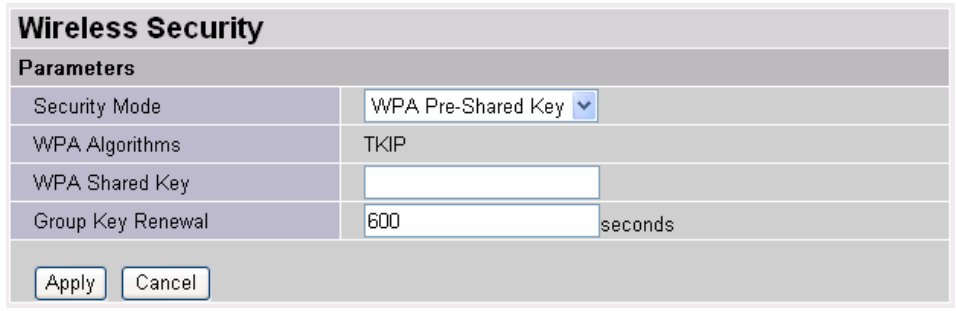
Connected: true or false. That it is the connection status between the system and the build-in wireless card.

AP Firmware Version: The Access Point firmware version.

Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network.
The default mode of wireless security is **disabled**.

WPA Pre-Shared Key

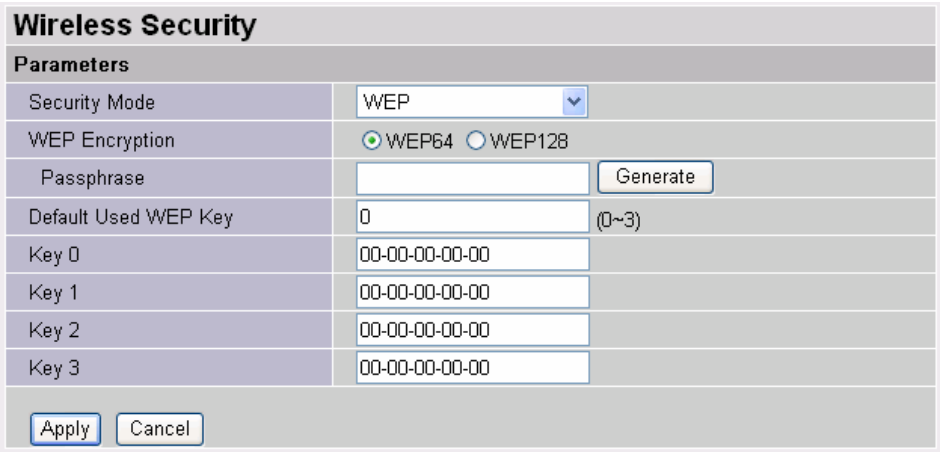


WPA Algorithms: TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

WEP



WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.

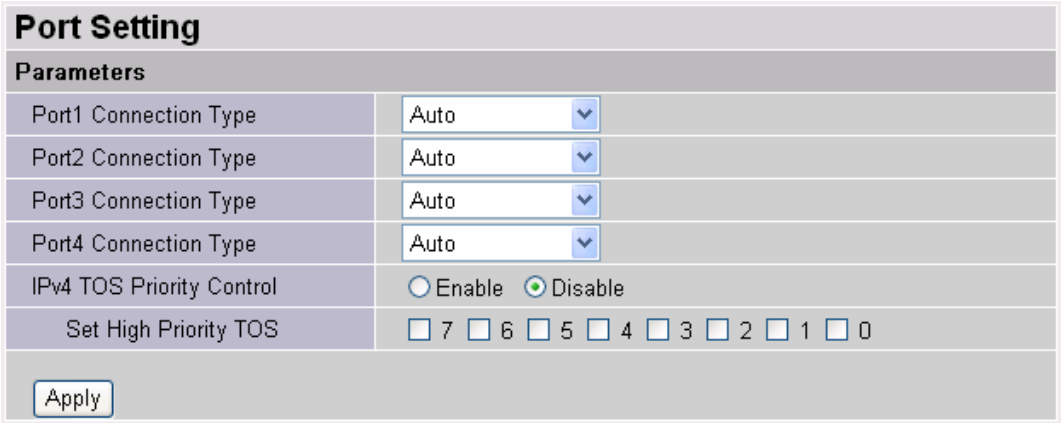
Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (0-3)** as below when the **Passphrase** is enabled.

Default Used WEP Key: Select the encryption key ID, please refer to **Key (0-3)** below.

Key (0-3): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



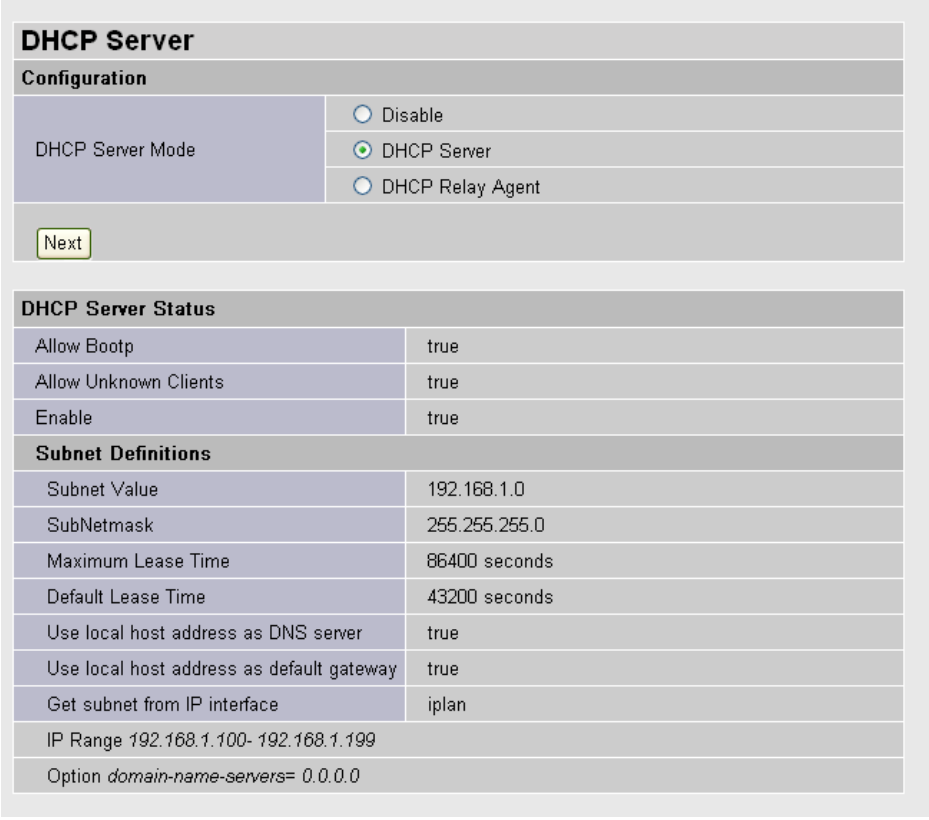
Port # Connection Type: Five options to choose from: Auto, 10M half-duplex, 10M full-duplex, 100M half-duplex or 100M full-duplex. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is **Auto**, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-2 are used to specify the priority (precedence) of the packet, and bits 3-5 are specified the delay, throughput and reliability.

This feature uses bits 0-2 to classify the packet's priority. If the packet is high priority, it will flow first. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the Precedence of TOS field matches the checked values in the table (0 to 7), this packet will be treated as high priority.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.



To disable the router's DHCP Server, check **Disabled** and click **Next,** then click **Apply.** When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PCs on your network, and set the default gateway for each PCs to the IP address of the router (by default this is 192.168.0.254).

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check **"Use Router as a DNS Server"**, the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

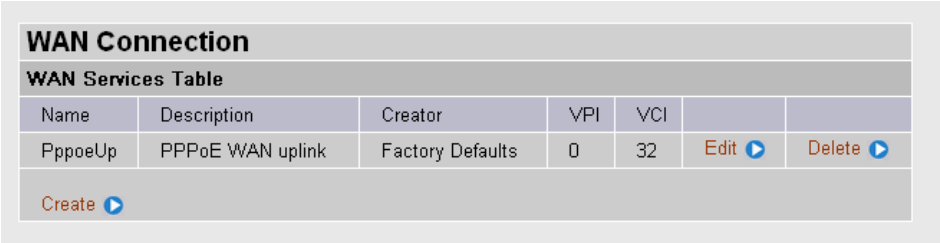
If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

Click **Apply** to enable this function.

WAN (Wide Area Network)

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet. There are two items within the **WAN** section: **ISP**, **DNS** and **ADSL**.

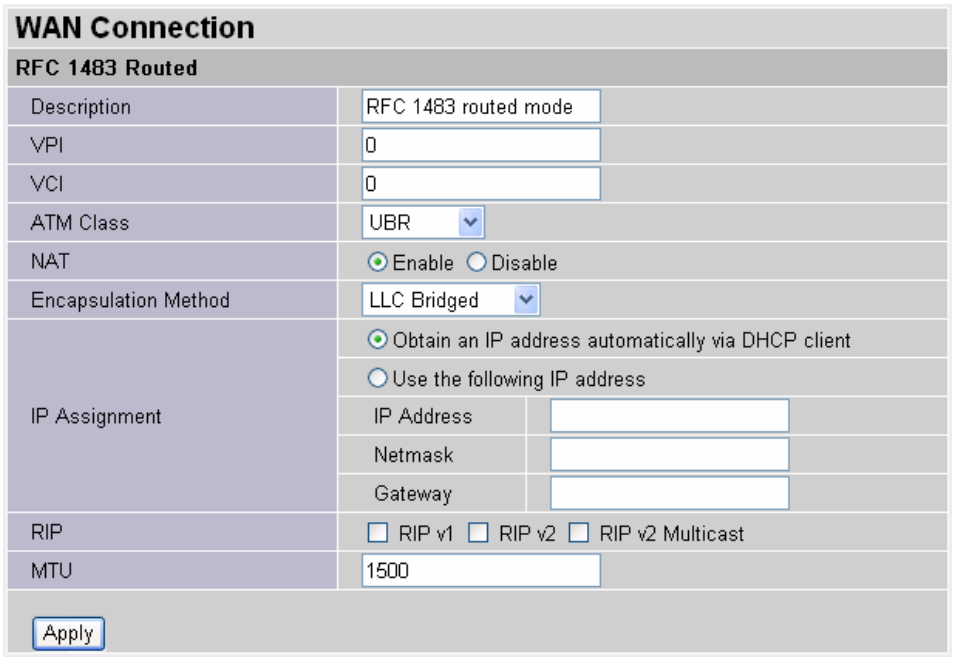
ISP



The factory default is PPPoE. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use PPPoE, you can delete the default WAN connection entry by clicking **Delete**. You may then click **Create** to create a connection to your ISP to surf the Internet.

A simpler alternative is to delete the current WAN connection entry then select **Quick Start** from the main menu on the left. Please see the Quick Start section of the manual for more information.

RFC 1483 Routed Connections



Description: Your description of this connection.

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

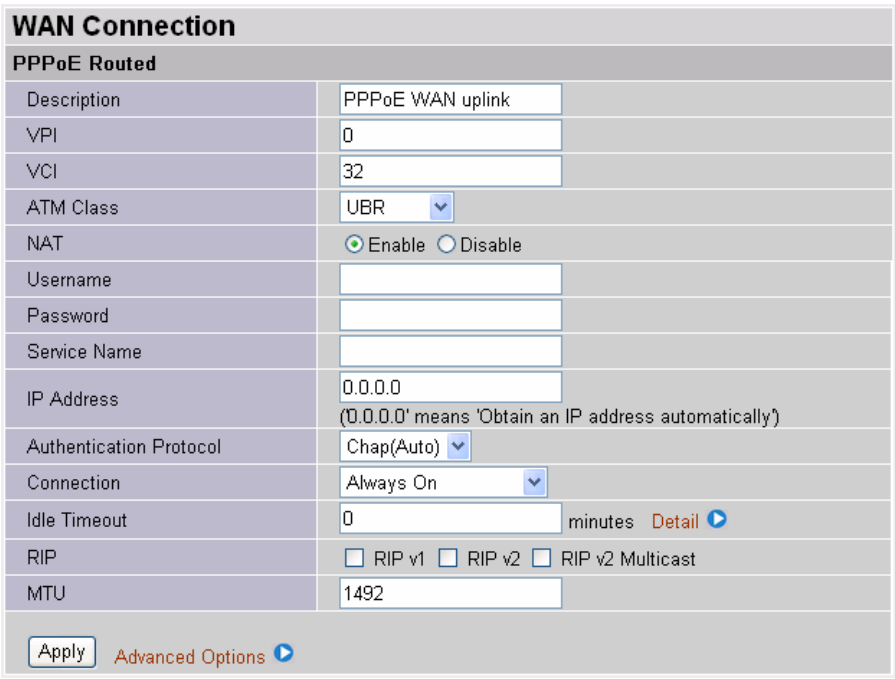
Encapsulation method: Select the encapsulation format, the default is LlcBridged. Select the one provided by your ISP.

DHCP client: Enable or disable the DHCP client, specify if the Router can get an IP address from the Internet Service Provider (ISP) automatically or not. Please click **Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE Connections



Description: A user-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is **Chap(Auto**). Your ISP will advise you whether to use **Chap** or **Pap.**

Connection:

⊙ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

⊙ **Connect to Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoE)

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU : Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNSto Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNSto Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

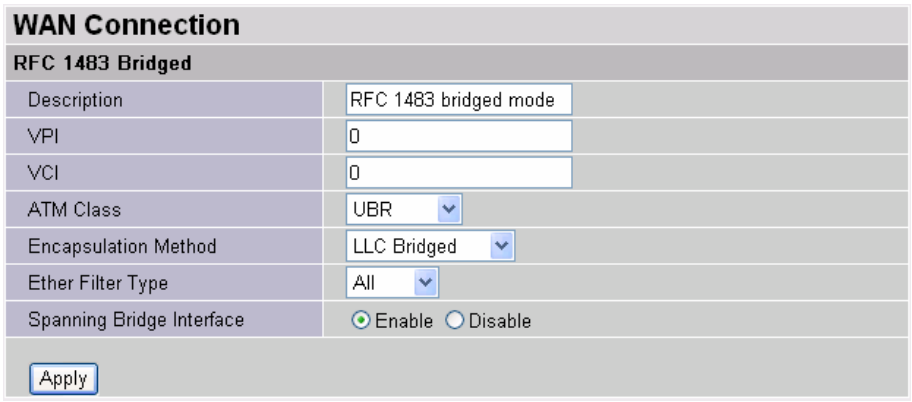
Give DNSto DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

RFC 1483 Bridged Connections



VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

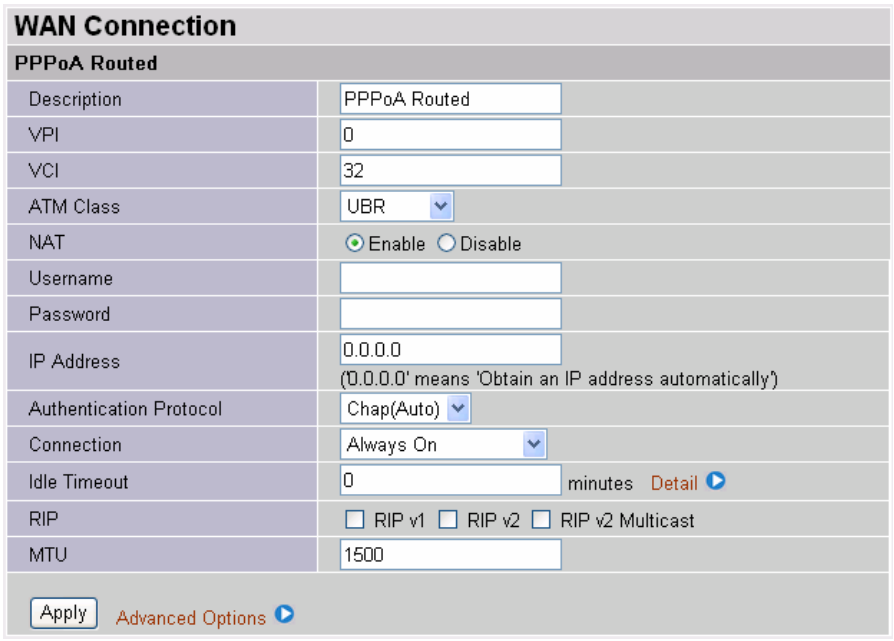
Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Ether Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

Spanning Bridge Interface: Enable/Disable spanning tree function of modem.

PPPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

IP Address: Specify an IP address allowed to logon and access the router's web server.. Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.

Authentication Protocol Type: Default is **Chap (Auto)**. Your ISP will advise you whether to use **Chap** or **Pap.**

Connection:

⊙ **Always on:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

⊙ **Connect to Demand:** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoA)

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU : Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNSto Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNSto Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

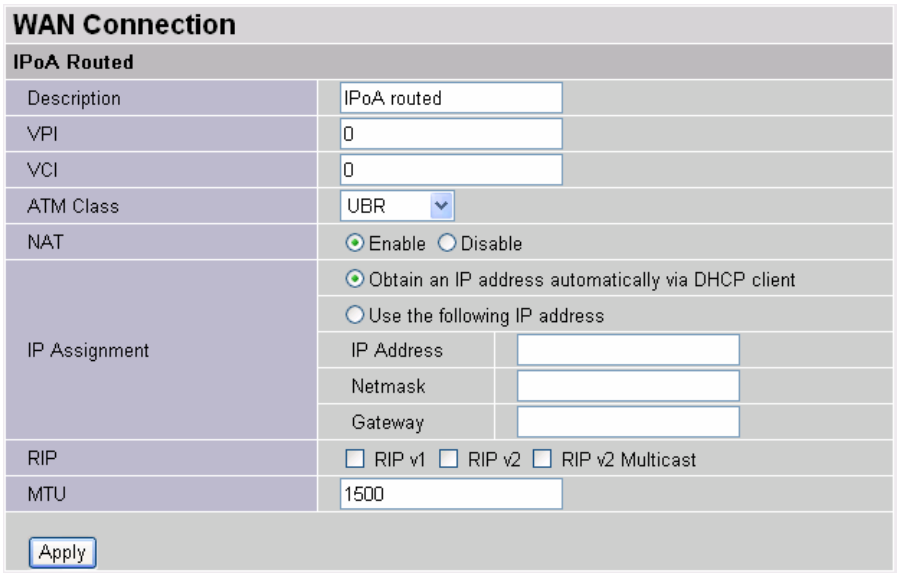
Give DNSto DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

IPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

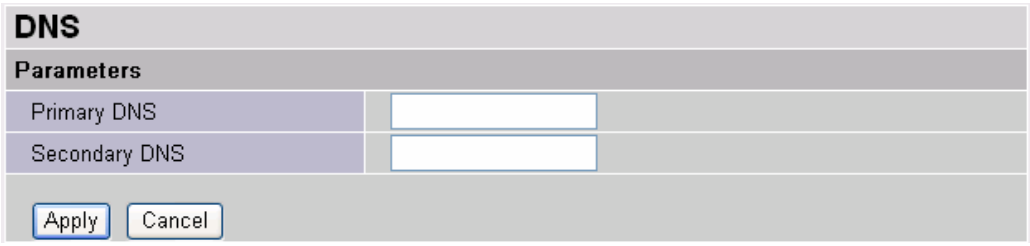
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

DHCP client: Enable or disable the DHCP client, specifying if the router can obtain an IP address from the Internet Service Provider (ISP) automatically or not. Please click **Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click **Specify an IP address** to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

DNS

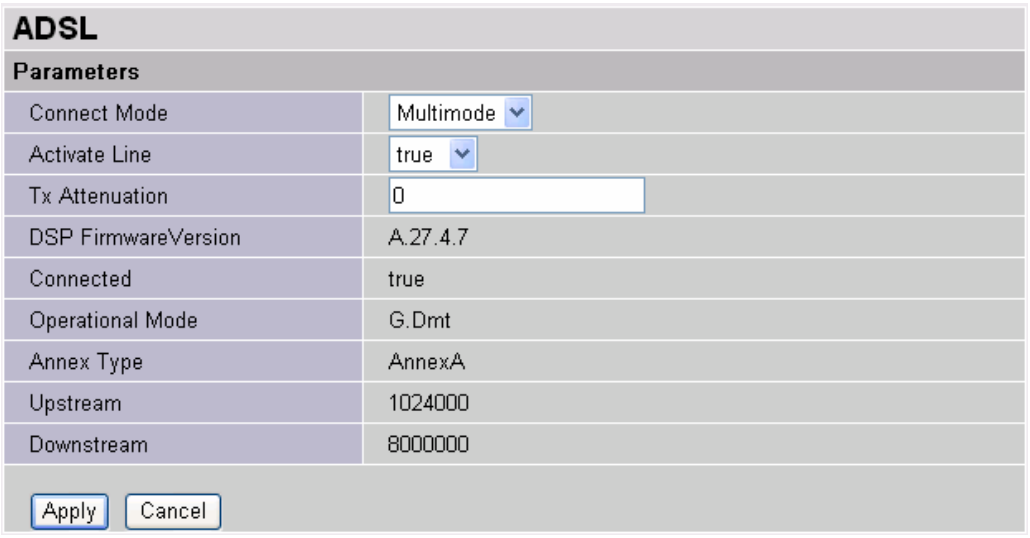


A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.TeleWell.com and an IP address. An IP address is a 32-bit number in the form of *xxx.xxx.xxx.xxx*, for example 192.168.0.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave the configuration field blank. Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

If you choose one of the other three protocols ▫ RFC1483 Routed/Bridged and IPoA check with your ISP, it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

ADSL



Connect Mode: The default is Multimode; it will detect the ADSL line code, G.dmt, G.lite, and T1.413 automatically. But in some area, it cannot detect the ADSL line code well. At this time, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.

Activate Line: Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of **Connect Mode**.

Tx Attenuation: Setting ADSL transmission gain, the value is between 0~12.

DSP FirmwareVersion: Current ADSL line code firmware version.

Connected: Display current ADSL line sync status.

Operational Mode: Display current ADSL mode standard (Operational Mode) your Router is using when ADSL line has sync.

Annex Type: ADSL Annex A, which works over a standard telephone line. Annex B, which works over an ISDN line.

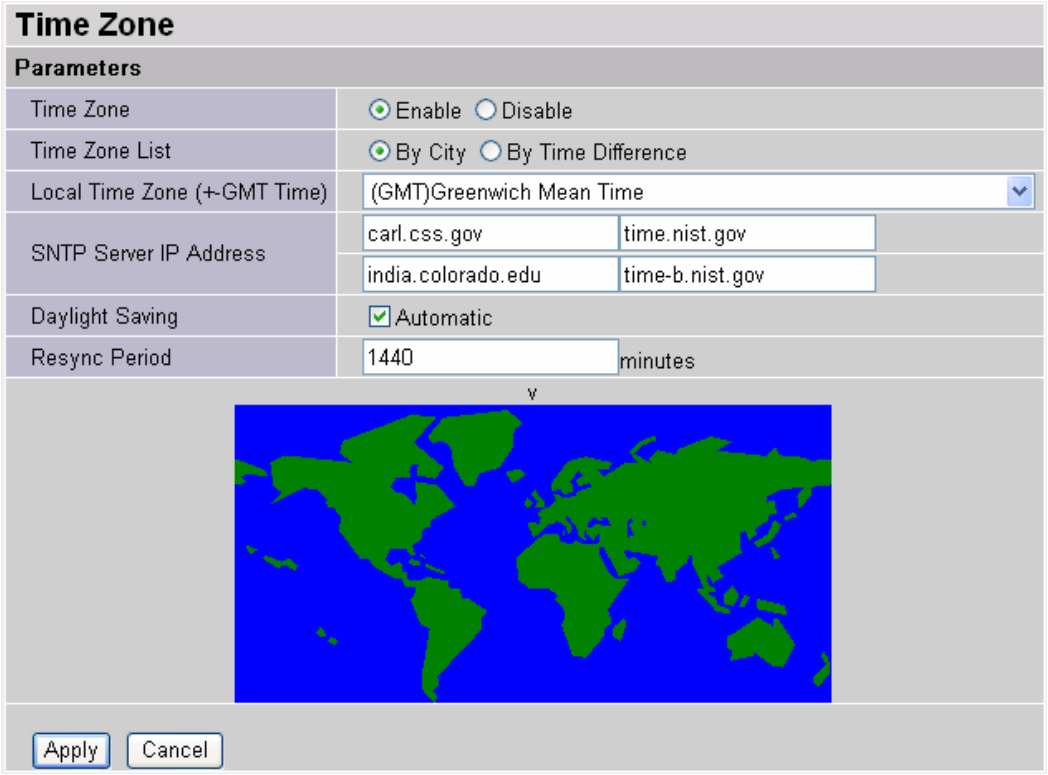
Upstream: Display current upstream rate of your ADSL line.

Downstream: Display current downstream rate of your ADSL line.

System

There are six items within the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart** and **User Management.**

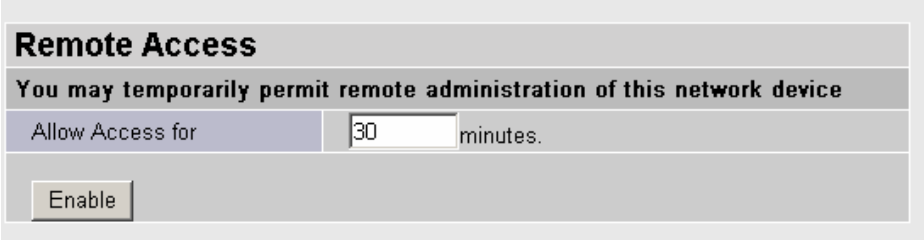
Time Zone



The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Poll Interval (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

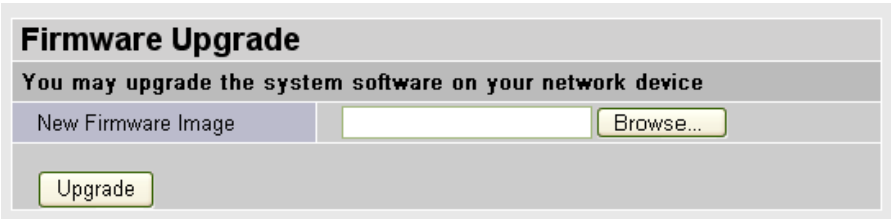
Remote Access



To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable.** You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of 0 minutes.

Firmware Upgrade



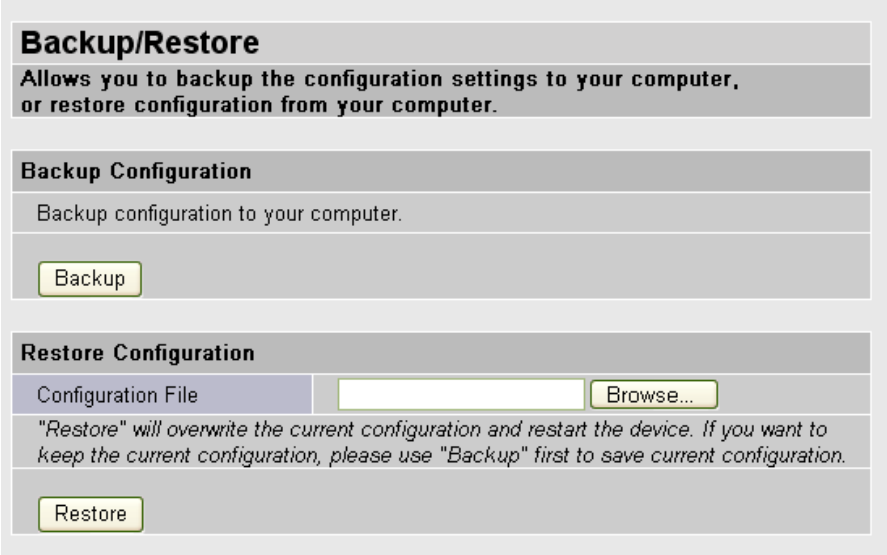
Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your TeleWell router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

Poistettu: <sp>

✓ DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore


Backup/Restore
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse...
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

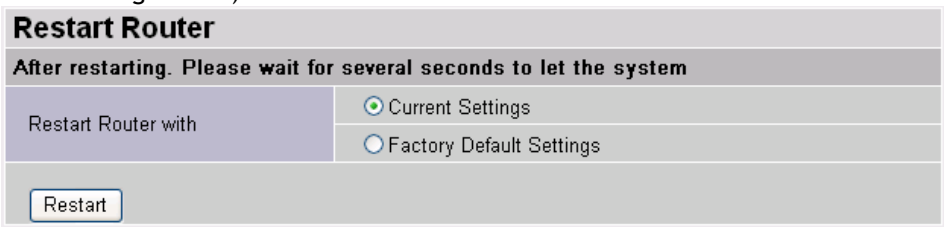
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

Restart Router

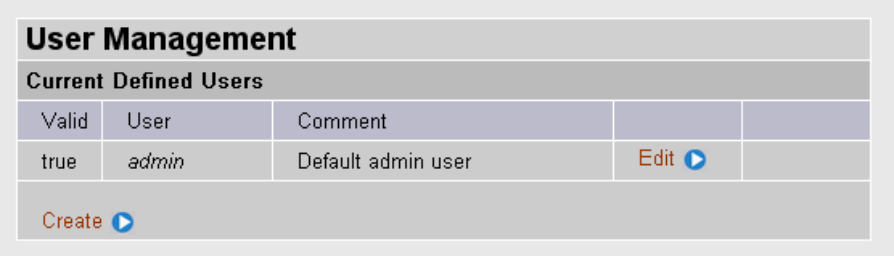
Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select *Factory Default Settings* to reset to factory default settings.

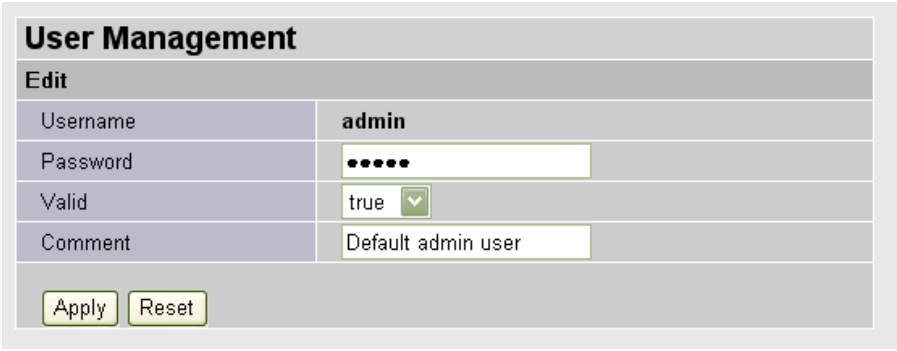
You may also reset your router to factory settings by holding the small Reset pinhole button on the back of your router in for 10-12 seconds whilst the router is turned on.

User Management



In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit,** you are shown the following options:

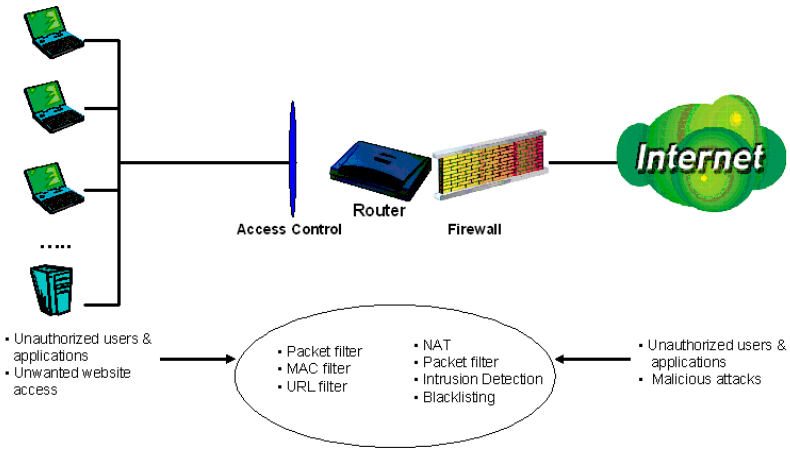


You can change the user's **password**, whether their account is active and **Valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account, however you can delete any other created accounts by clicking **Delete** when editing the user.

You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation. Please see the **WAN** configuration section for more details on NAT) the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



Firewall & Filter

Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when NAT function is enabled.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing your local network from the Internet.

> NOTE: *When using Virtual Servers your PCs will be exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.*

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevents access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.

MAC Filter rules: To prevent unauthorized computers accessing the Internet.

URL Filter: To block PCs on your local network from unwanted websites.

You can find six items under the **Firewall** section: **General Settings, Packet Filter, Intrusion Detection, MAC Address Filter, URL Filter** and **Firewall Log.**

General Settings

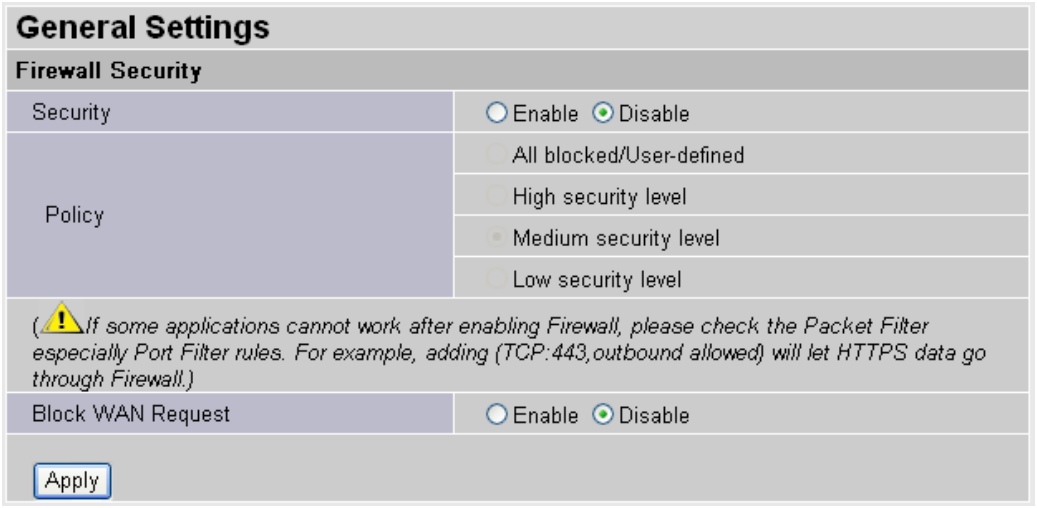
You can choose not to enable Firewall, to add all filter rules by yourself, or enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is divided into two sections: Port Filters and Address Filters, used to filter packets based-on Applications (Port) or IP addresses.

There are four options when you enable the Firewall, they are:

- All blocked/User-defined: no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- High/Medium/Low security level: the pre-defined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either **High, Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filters that changes between each setting.

If you choose of the preset security levels and then add custom filters, you may temporarily disable the firewall and recover your custom filter settings by re-selecting the same security level.



The **"Block WAN Request"** is a stand-alone function and not relate to whether security enable or disable. Mostly it is for preventing any scan tools from WAN site by hacker.

Packet Filter

Packet Filter

Firewall Security

Type	Configuration		Note
external < > internal	Port Filters	Address Filters	1. By default, all protocol types and TCP/UDP ports are blocked. 2. Only the listed IP addresses are blocked

Port Filters

The pre-defined port filter rules for High, Medium and Low security levels are listed. See Table 1.

Table 1: Pre-defined Port Filter

Application	Protocol	Port Number		Firewall - High		Firewall - Medium		Firewall - Low	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	**YES**	NO	**YES**	NO	**YES**
DNS (53)	UDP(17)	53	53	NO	**YES**	NO	**YES**	**YES**	**YES**
DNS (53)	TCP(6)	53	53	NO	**YES**	NO	**YES**	**YES**	**YES**
FTP(21)	TCP(6)	21	21	NO	NO	NO	**YES**	NO	**YES**
Telnet(23)	TCP(6)	23	23	NO	NO	NO	**YES**	NO	**YES**
SMTP(25)	TCP(6)	25	25	NO	**YES**	NO	**YES**	NO	**YES**
POP3(110)	TCP(6)	110	110	NO	**YES**	NO	**YES**	NO	**YES**
NEWS(119)	TCP(6)	119	119	NO	NO	NO	**YES**	NO	**YES**
RealAudio (7070)	UDP(17)	7070	7070	NO	NO	**YES**	**YES**	**YES**	**YES**
PING	ICMP(1)	N/A	N/A	NO	**YES**	NO	**YES**	NO	**YES**
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	**YES**	**YES**	**YES**
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	**YES**	**YES**	**YES**
SSH(22)	TCP(6)	22	22	NO	NO	NO	**YES**	**YES**	**YES**
NTP(123)	UDP(17)	123	123	NO	**YES**	NO	**YES**	NO	**YES**
HTTPS(443)	TCP(6)	443	443	NO	NO	NO	**YES**	NO	**YES**
ICQ (5190)	TCP(6)	5190	5190	NO	NO	NO	**NO**	**YES**	**YES**

Inbound: Internet to LAN
Outbound: LAN to Internet.

Address Filters

Address Filters are used to block traffic to/from particular IP addresses. They can be used to block IP addresses either on the Internet or on your local network. There are no pre-defined address filter rules; you can add the filter rules to meet your requirements. There are two kinds of address filters, one is inbound, and the other is outbound. The rules can be set to prevent unauthorized users (hosts or network) to access the Internet from LAN (outbound) and/or access LAN from the Internet (inbound).

Host IP Address: This is the IP address you wish to block access to or from.

Host Subnet Mask: This is the subnet mask for the IP address range you wish to block.

Direction: Whether you want to block access to the Internet (**"outbound"**), from the Internet (**"inbound"**) or both to and from the Internet (**"both"**).

Tip: To block access to/from a single IP address, enter that IP address as the **Host IP Address** and use a **Host Subnet Mask** of "255.255.255.255".

Example: Configuring your firewall to allow for a publicly accessible web server on your LAN

The pre-defined port filter rule for HTTP (TCP port 80) is the same no matter whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High), inbound HTTP access is not allowed.

Port Filters

Filtering Rules

Add TCP/UDP Filter | Add Raw IP Filter | Return

Filtering Table

Type	Start Port	End Port	Inbound	Outbound		
TCP	80	80	Block	Allow	Edit	Delete
UDP	53	53	Block	Allow	Edit	Delete
TCP	53	53	Block	Allow	Edit	Delete
TCP	21	21	Block	Allow	Edit	Delete
TCP	23	23	Block	Allow	Edit	Delete
TCP	25	25	Block	Allow	Edit	Delete
TCP	110	110	Block	Allow	Edit	Delete
TCP	119	119	Block	Allow	Edit	Delete
UDP	7070	7070	Allow	Allow	Edit	Delete
ICMP	N/A	N/A	Block	Allow	Edit	Delete
TCP	1720	1720	Block	Allow	Edit	Delete
TCP	1503	1503	Block	Allow	Edit	Delete
TCP	22	22	Block	Allow	Edit	Delete
UDP	123	123	Block	Allow	Edit	Delete
TCP	443	443	Block	Allow	Edit	Delete

Configuring Packet Filter

1. Click Packet Filter - you will get the following page:

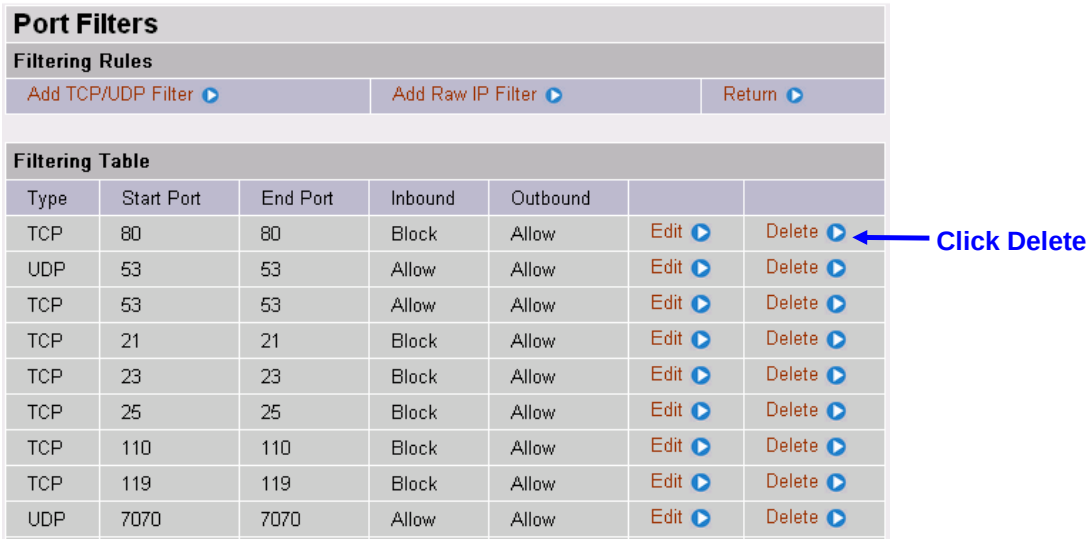
Click Port Filters

Packet Filter

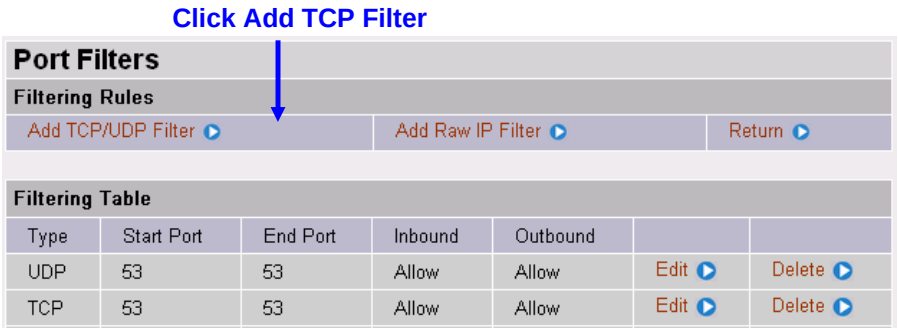
Firewall Security

Type	Configuration		Note
external < > internal	Port Filters	Address Filters	1. By default, all protocol types and TCP/UDP ports are blocked. 2. Only the listed IP addresses are blocked

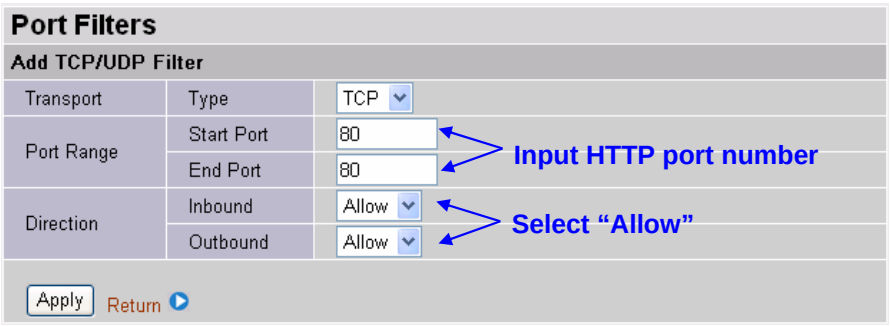
2. Click **Port Filters**. You will then be presented with the pre-defined port filter rules screen (in this case for the low security level), shown below:


Port Filters
Filtering Rules
Add TCP/UDP Filter
Add Raw IP Filter
Return
Filtering Table
Type Start Port End Port Inbound Outbound
TCP 80 80 Block Allow Edit Delete
UDP 53 53 Allow Allow Edit Delete
TCP 53 53 Allow Allow Edit Delete
TCP 21 21 Block Allow Edit Delete
TCP 23 23 Block Allow Edit Delete
TCP 25 25 Block Allow Edit Delete
TCP 110 110 Block Allow Edit Delete
TCP 119 119 Block Allow Edit Delete
UDP 7070 7070 Allow Allow Edit Delete
Click Delete

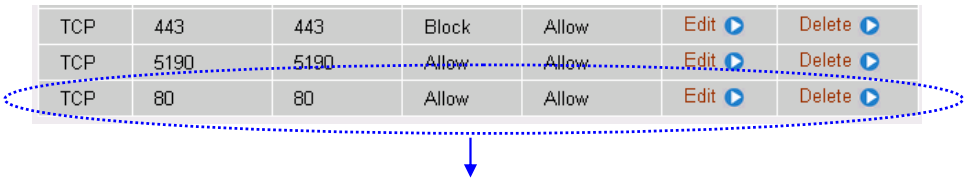
3. Click **Delete** to delete the existing HTTP rule.
4. Click **Add TCP Filter**.



5. Input the port number (80) and set both **Inbound** & **Outbound** to **Allow**.



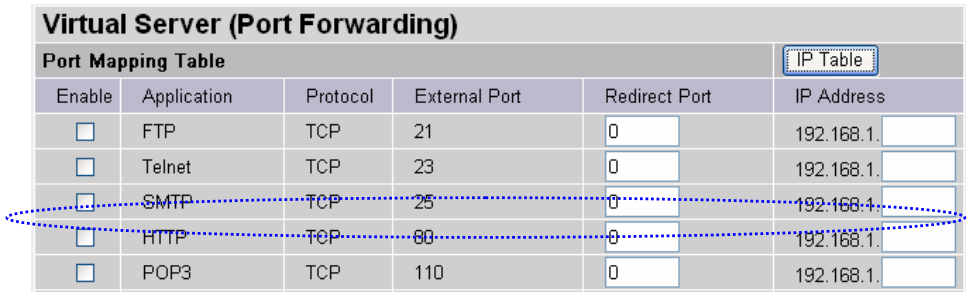
6. The new port filter rule for HTTP is shown below:



TCP	443	443	Block	Allow	Edit	Delete
TCP	5190	5190	Allow	Allow	Edit	Delete
TCP	80	80	Allow	Allow	Edit	Delete

HTTP inbound & outbound application

7. Configure your Virtual Server ("port forwarding") settings so that incoming HTTP requests on port 80 will be forwarded to the PC running your web server:



Virtual Server (Port Forwarding)

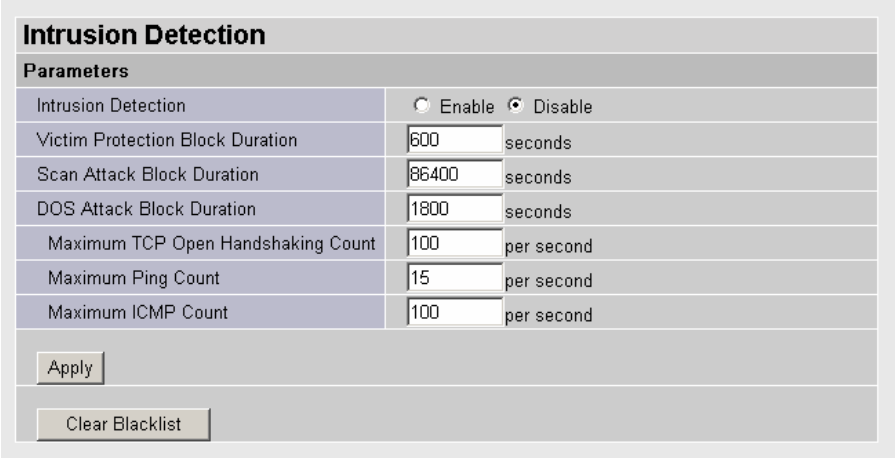
Port Mapping Table — IP Table

Enable	Application	Protocol	External Port	Redirect Port	IP Address
☐	FTP	TCP	21	0	192.168.1.
☐	Telnet	TCP	23	0	192.168.1.
☐	SMTP	TCP	25	0	192.168.1.
☐	HTTP	TCP	80	0	192.168.1.
☐	POP3	TCP	110	0	192.168.1.

To enable the HTTP service in Virtual Server settings, input the web server PC's IP address.

Tip: If you wish to setup permanent remote management of your router, you may enter the router's IP instead.

Intrusion Detection



The router's *Intrusion Detection System* (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is false (disabled). Some attack types are denied immediately without using the Blacklist function, such as *Land attack* and *Echo/CharGen scan*.

Block Duration:

- **DoS Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.
- **Scan Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.
- **Victim Protection Block Duration**: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.

Victim Protection: If enabled, IDS will block Smurf attack attempts. Default is false.

Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

For *SYN Flood*, *ICMP Echo Storm* and *ICMP flood*, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

Table 2: Hacker attack types recognized by the IDS

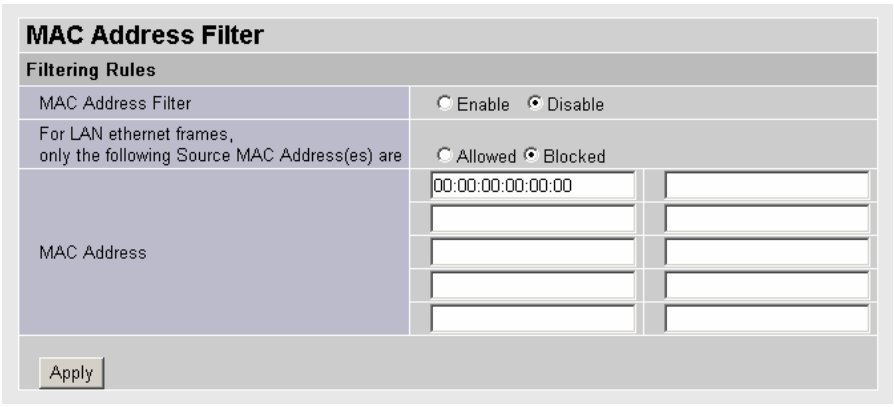
Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

MAC Address Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the switch to only accept traffic from specified machines, or else to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements



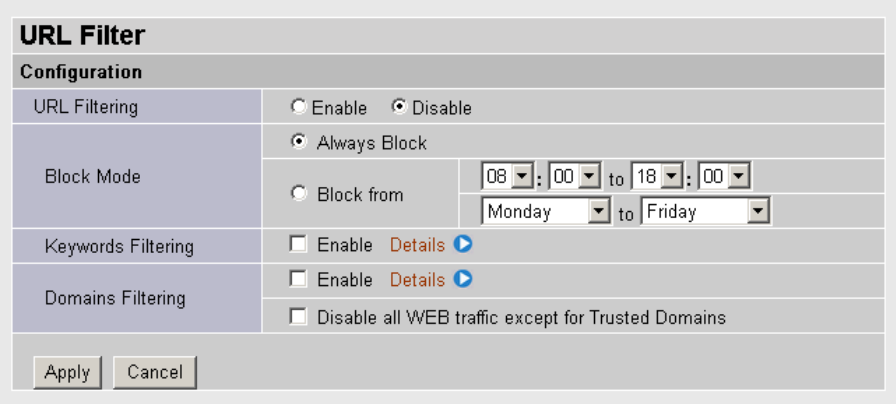
Enable/Disable: To enable or disable the MAC Address Filter function.

Allowed/Blocked: To allow or block the following MAC addresses to surf outside network only. If you check **Allowed**, please be sure your PC's MAC address is listed. If you check **Blocked**, please be sure your PC's MAC address is not listed.

MAC Address: There are 10 entries to enter the MAC addresses you want manage.

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.TeleWell.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



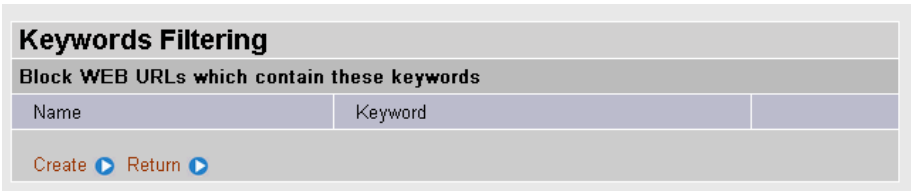
Enable/Disable: To enable or disable URL Filter feature.

Always Block: Select to always check the URL filter rules (i.e. at all hours of the day).

Block from: Specify the time period to check the URL filter rules (e.g. during work hours).

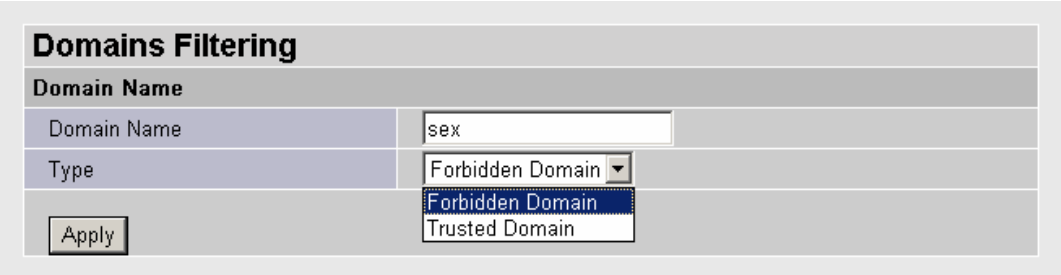
Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif"). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

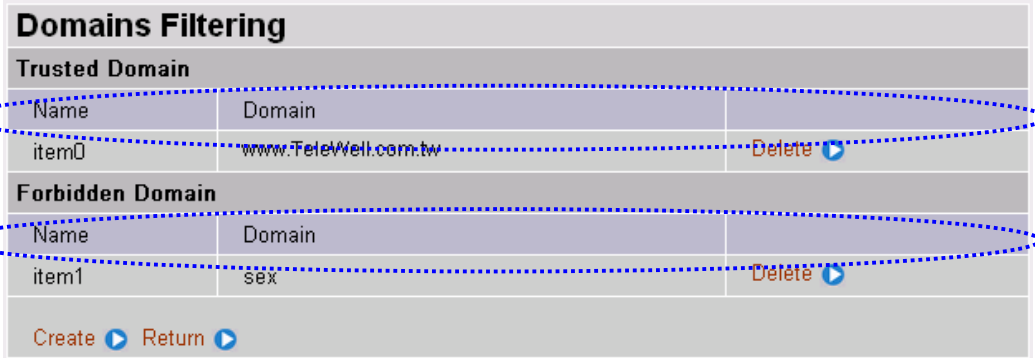
For example, if the URL is http://www.TeleWell.com.tw/abcde.html, it will be dropped as the keyword "abcde" occurs in the URL.



Domains Filtering: This function checks the domain name in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list, and if present then the connection attempt is dropped..
3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the domain only should be specified, not the full URL. For example to block traffic to www.sex.com, enter "sex" or "sex.com" instead of "www.sex.com". In the example below, the URL request for www.TeleWell.com.tw will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.sex or www.sex.com will be dropped, because TeleWell.com is in the forbidden list.

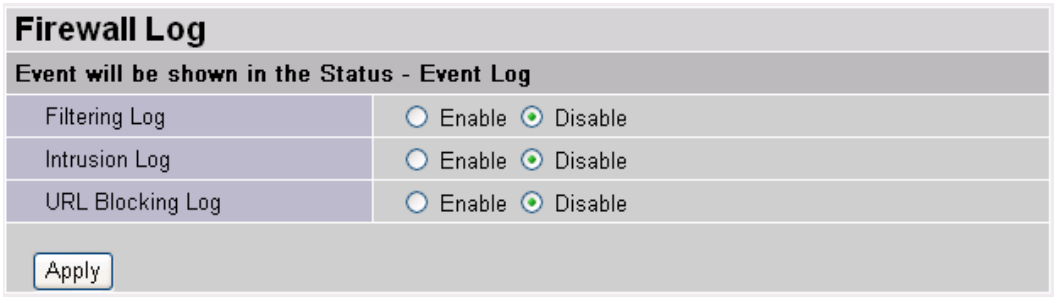




Restrict URL Features:

- **Block Java Applet:** This function can block Web content which including the Java Applet. It is for preventing someone who wants to damage your system via standard HTTP protocol.
- **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping **Domains Filtering** function.

Firewall Log



Firewall Log display log information of any unexpected action with your firewall settings.

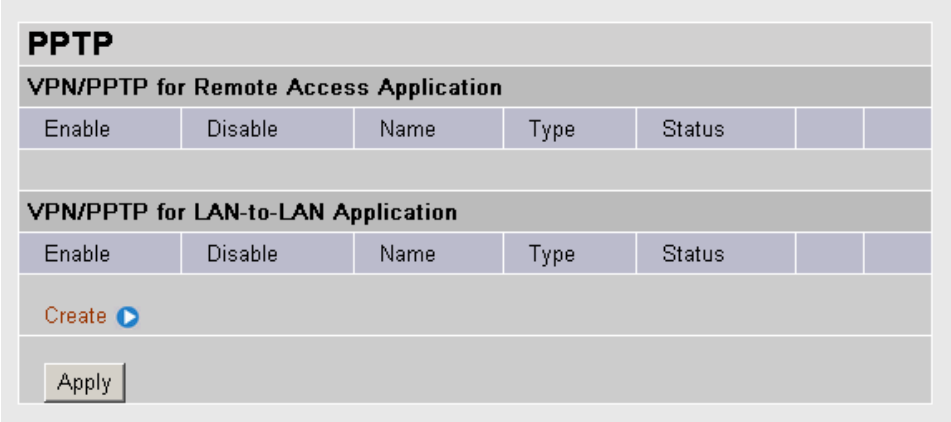
Check the **Enable** box to activate the logs.

Log information can be seen in the **Status – Event Log** after enabling.

VPN (Virtual Private Networks)

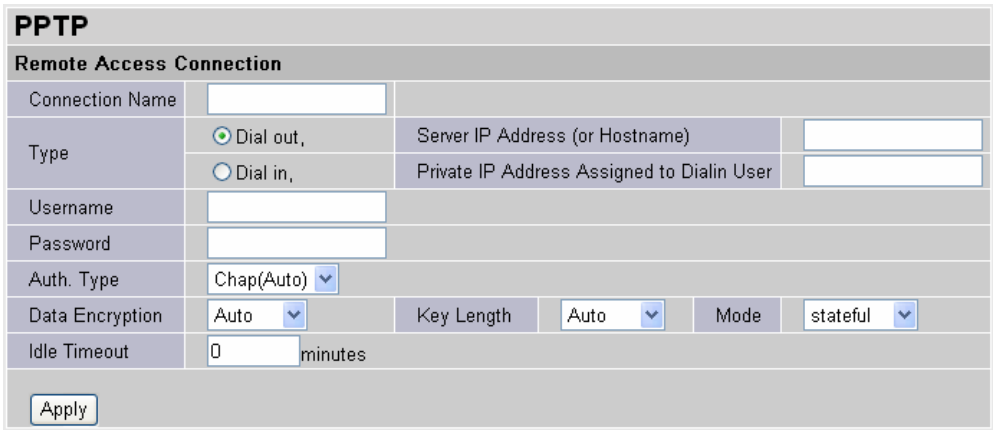
Your router support three main types of VPN (Virtual Private Network), **PPTP**, **IPSec** and **L2TP**, and these are the two major section choices from the menu on the left.

PPTP



There are two types of PPTP VPN supported, **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to configure a new VPN connection.

Remote Access PPTP Connection



Connection Name: This allows you to identify this particular connection, e.g. "Connection to office".

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

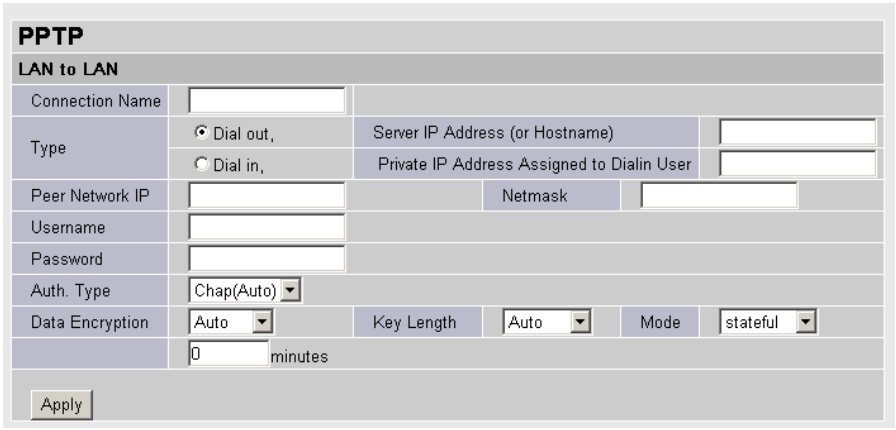
Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after changing settings.

LAN to LAN PPTP Connection



Connection Name: A user-define description of the connection.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router establish the connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server to accept incoming connections, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by the your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

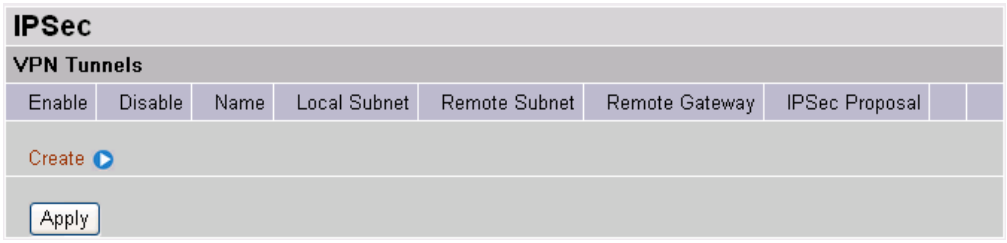
Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

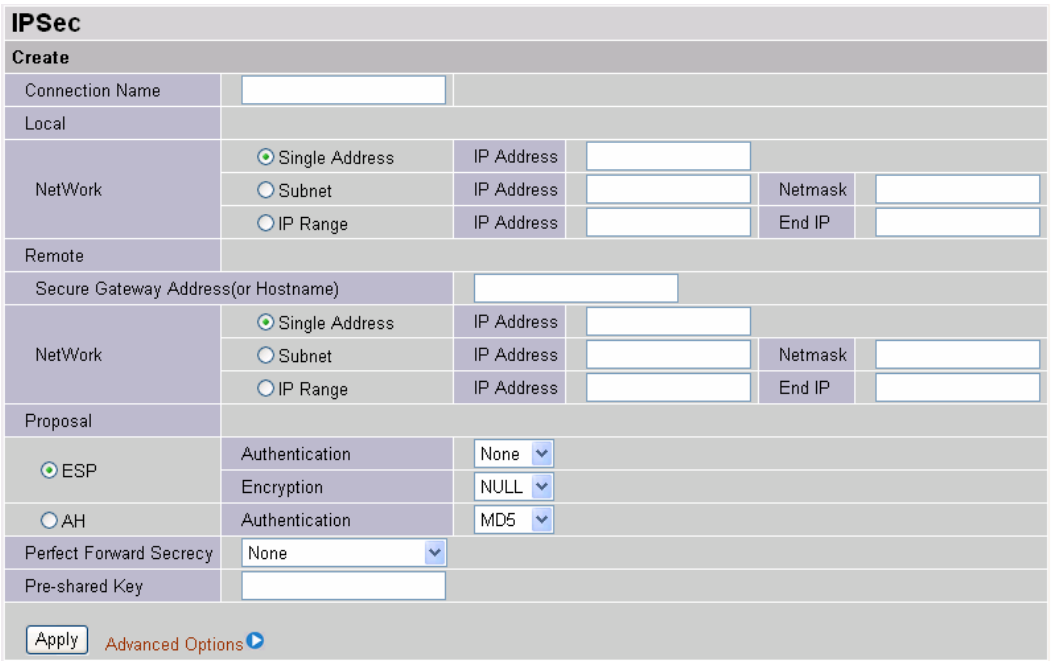
Click **Apply** after changing settings.

IPSec



Click **Create** to configure a new IPSec VPN connection.

Configure a new VPN Connection



Connection Name: A user-defined name for the connection (e.g. "connection to office").

Local:

Local Network: Set the IP address, subnet or address range of the local network.

⊙ **Single Address:** The IP address of the local host.

⊙ **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.0.254).

⊙ **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Remote:

Secure Gateway Address (or hostname): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Network: Set the IP address, subnet or address range of the remote network.

Proposal:

Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA-1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA-1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

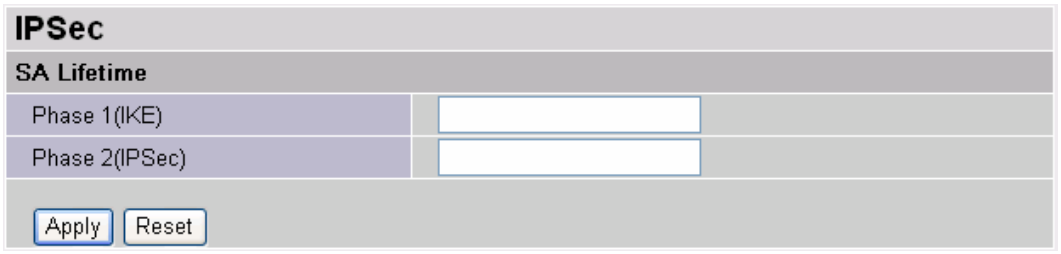
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Select the **Save** button to save the setting.

Advanced Option

Click **Advanced Option** to change the following settings:



SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

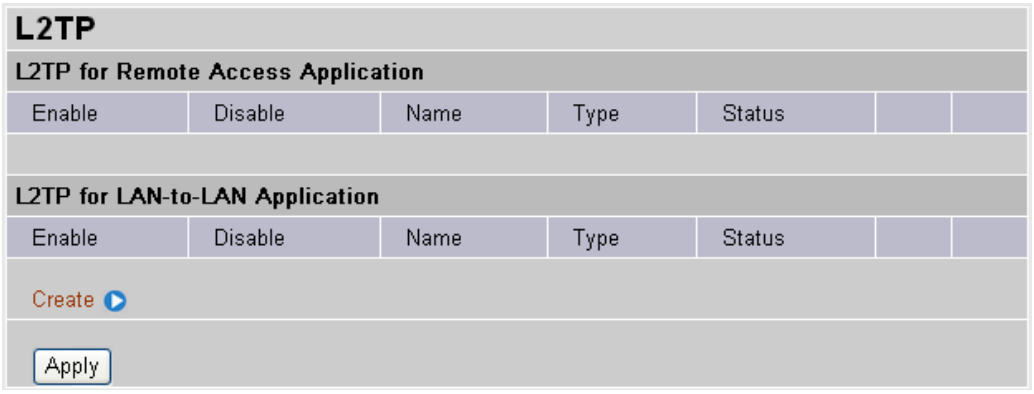
Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 240 minutes.

Phase 2 (IPSec): To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

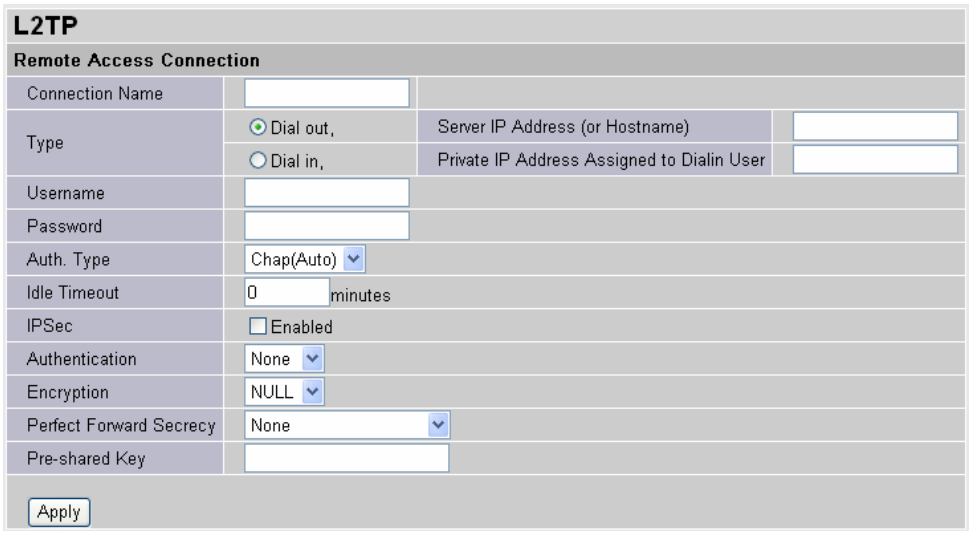
Select the **Apply** button to update the settings.

L2TP



There are two types of L2TP VPN supported, **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to configure a new VPN connection.

Remote Access L2TP Connection



Connection Name: This allows you to identify this particular connection, e.g. "Connection to office".

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after changing settings.

IPSec: Enable for enhancing your LT2P VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA-1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA-1:** A one-way hashing algorithm that produces a 160−bit hash.

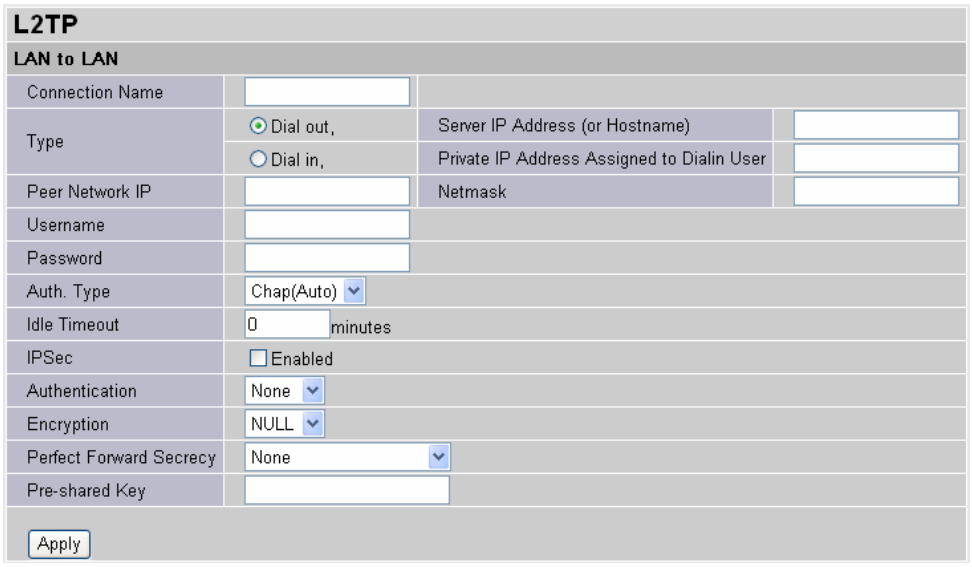
Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

LAN to LAN L2TP Connection



Connection Name: A user-define description of the connection.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router establish the connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server to accept incoming connections, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by the your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on. Click **Apply** after changing settings.

IPSec: Enable for enhancing your LT2P VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA-1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA-1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

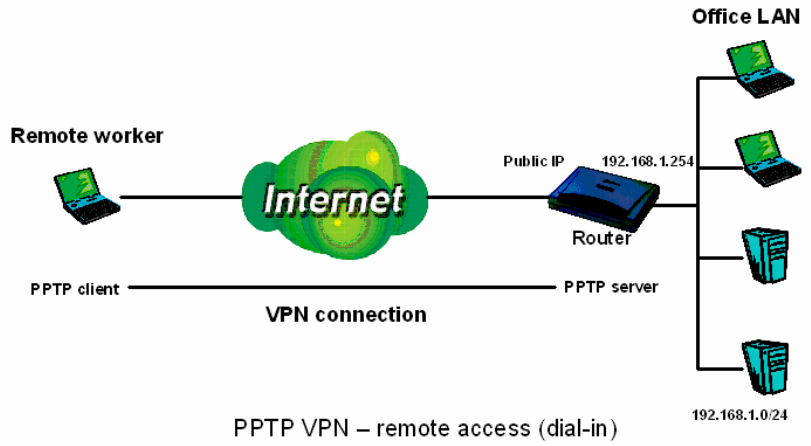
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Example: Configuring a Remote Access PPTP VPN Dial-in Connection

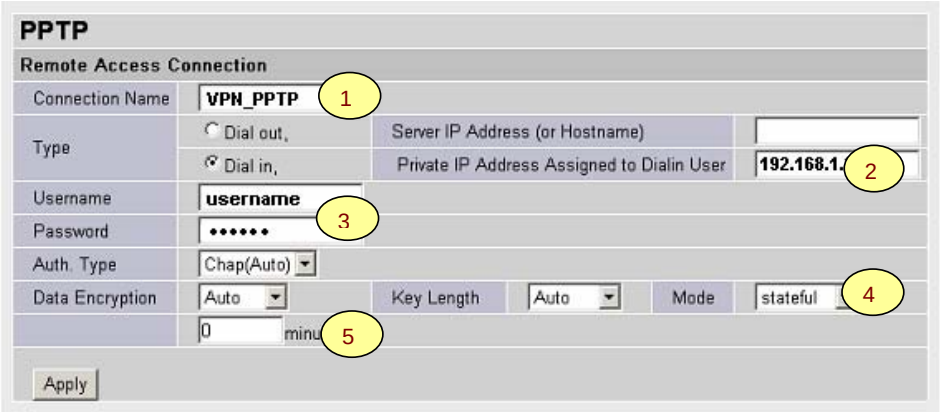
A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows 2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



PPTP VPN – remote access (dial-in)

Configuring PPTP VPN in the Office

The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

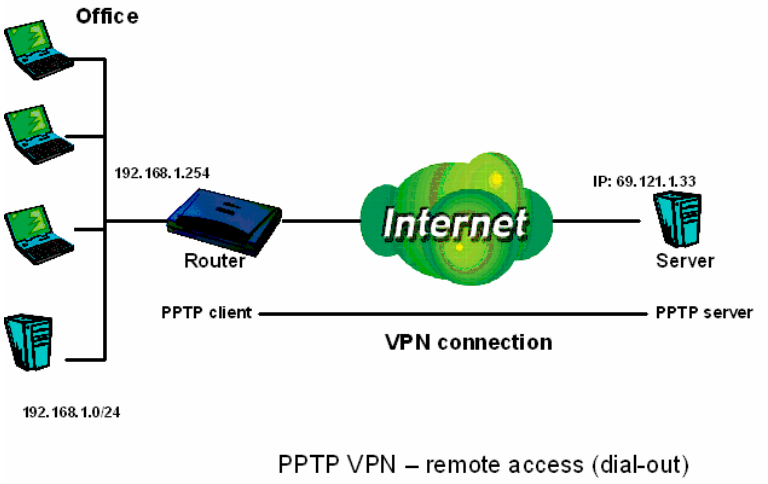


Item	Function		Description
1	Connection Name	VPN_PPTP	Given a name of PPTP connection
2	Dail in		Check Dial in
	Private IP Address Assigned to Dailin User	192.168.1.200	An assigned IP address for the remote worker
3	Username	username	Input username & password to authenticate remote worker
	Password	xxxxxx	

4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
5	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always-on.

Example: Configuring a Remote Access PPTP VPN Dial-out Connection

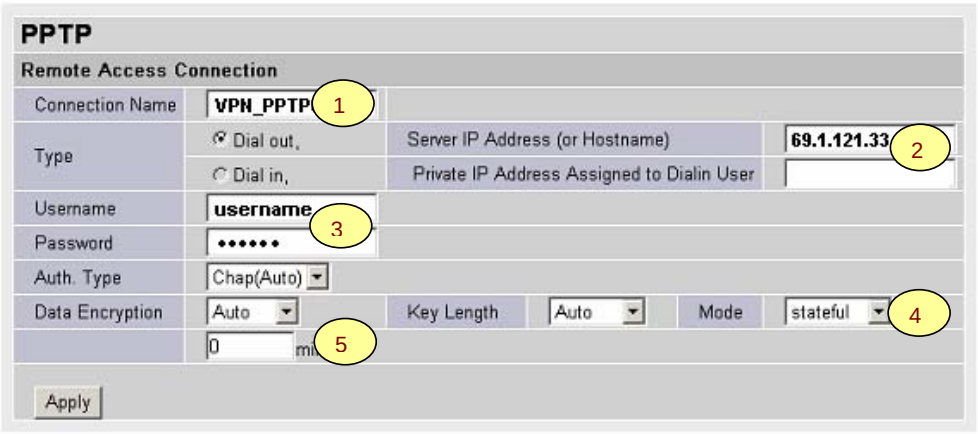
A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



PPTP VPN – remote access (dial-out)

Configuring the PPTP VPN in the Office

You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.

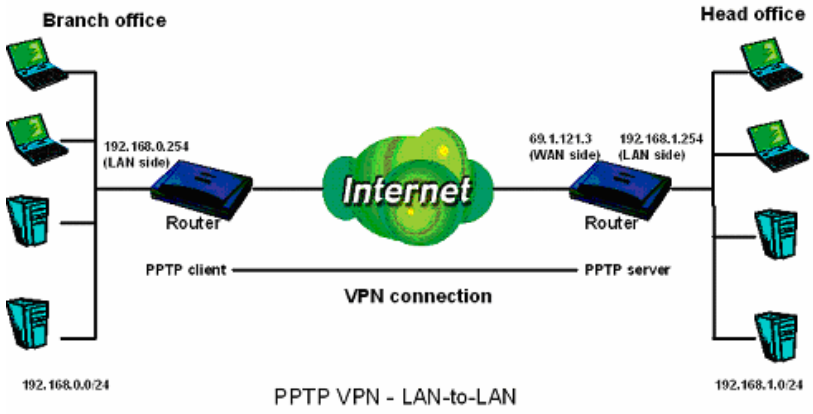


Item	Function		Description
1	Connection Name	VPN_PPTP0	Given name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.1.121.33	An Dialed server IP
3	Username	username	A given username & password
	Password	xxxxxx	
	Auth.Type	Chap(Auto)	Keep as default value in most of the cases,
	Data Encryption	Auto	

4	Key Length	Auto	PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Mode	stateful	
5	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always-on.

Example: Configuring a LAN-to-LAN PPTP VPN Connection

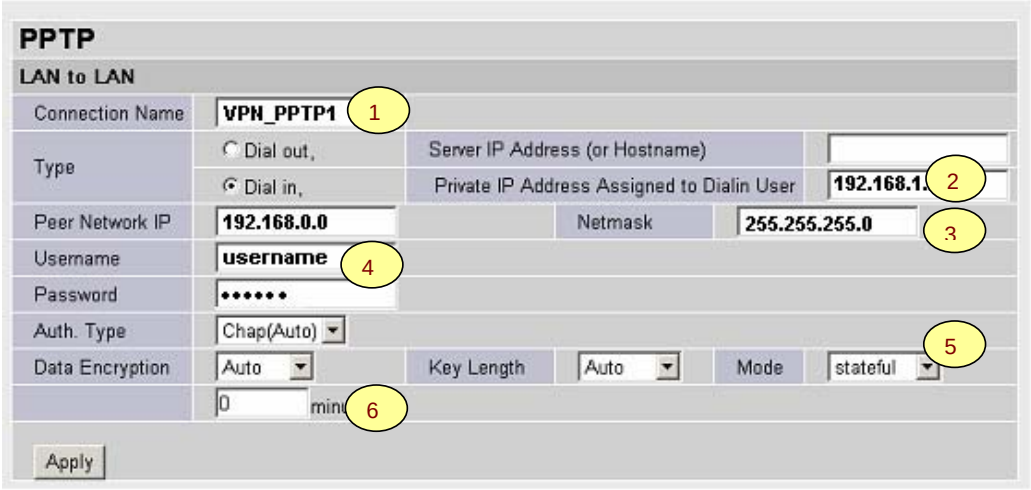
The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.



PPTP VPN - LAN-to-LAN

Configuring PPTP VPN in the Head Office

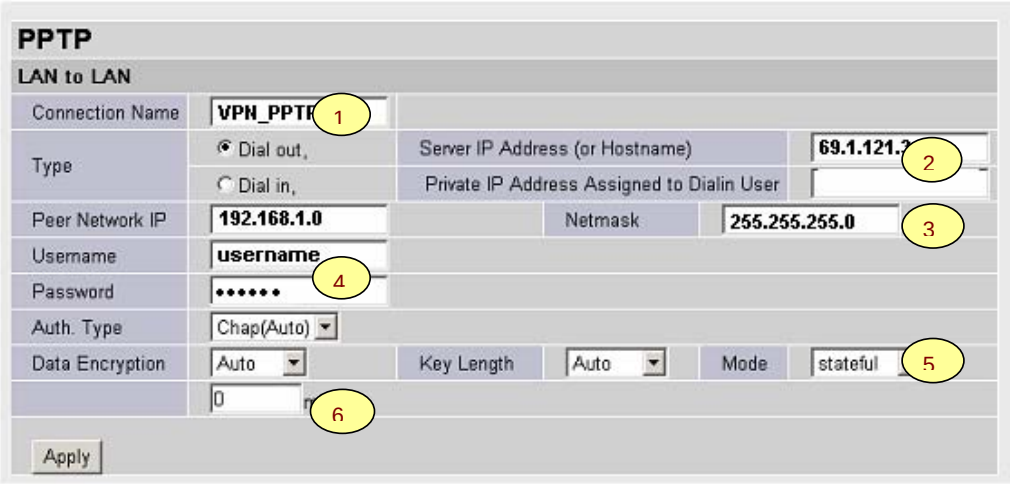
The IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Connection Name	VPN_PPTP1	Given a name of PPTP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialin User	192.168.1.201	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	Username	Input username & password to authenticate branch office network
	Password	xxxxxx	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always-on.

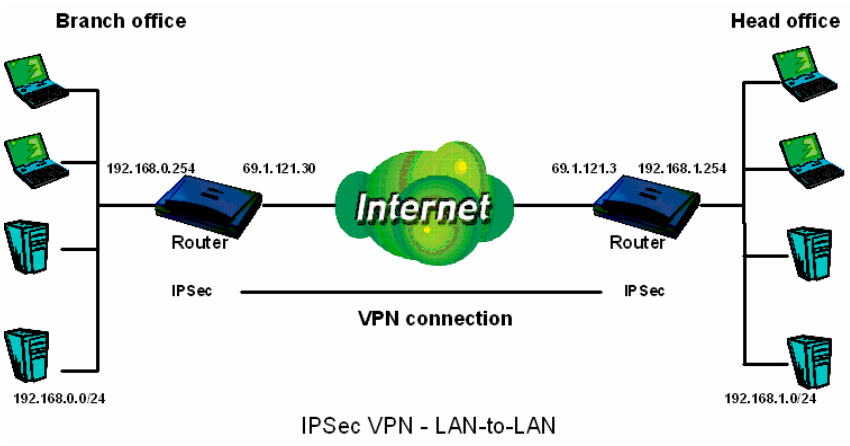
Configuring PPTP VPN in the Branch Office

The IP address 69.1.121.30 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Item	Function		Description
1	Connection Name	VPN_PPTP1	Given a name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.1.121.3	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	Username	Input username & password to authenticate branch office network
	Password	xxxxxx	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always-on.

Example: Configuring a IPSec LAN-to-LAN PPTP VPN Connection

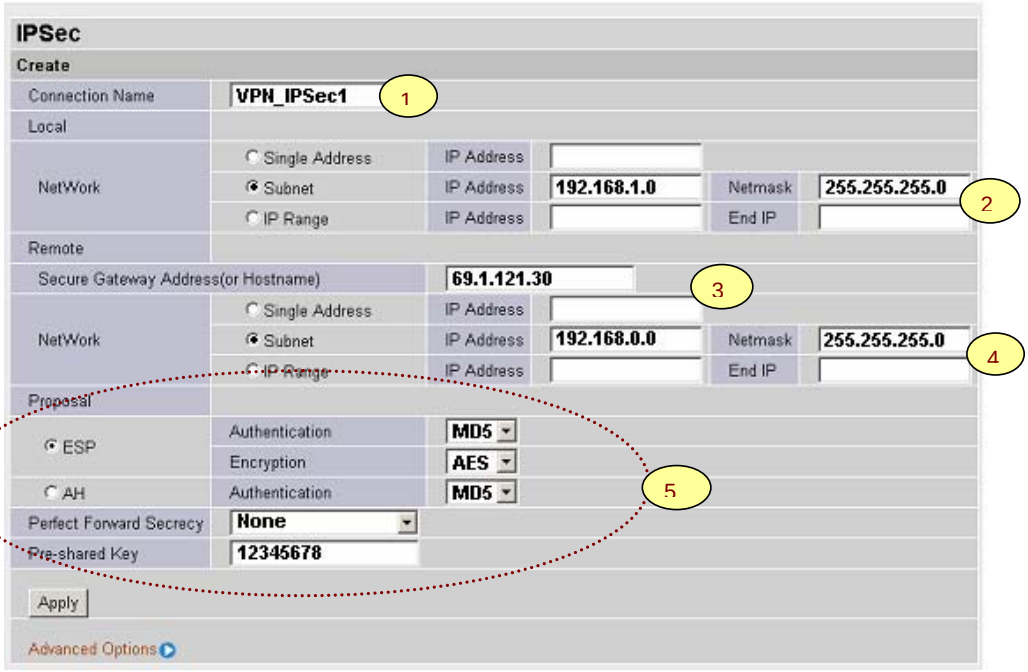


IPSec VPN - LAN-to-LAN

Table 3: Network Configuration and Security Plan

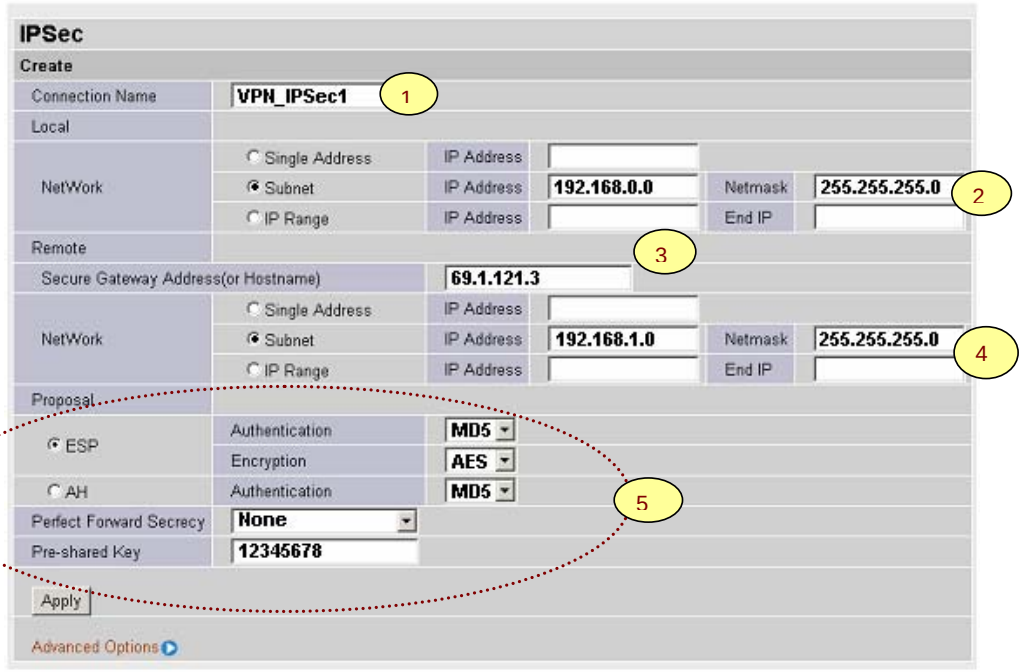
	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.1.121.30	69.1.121.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Configuring IPSec VPN in the Head Office



Item	Function		Description
1	Connection Name	VPN_IPSec1	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network (refer to Table 3)
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.1.121.30	IP address of the head office router (in WAN side)
4	Subnet		Check Subnet radio button
	IP Address	192.168.0.0	Branch office network (refer to Table 3)
	Netmask	255.255.255.0	
5	Authentication		Security plan (refer to Table 3)
	Encryption		
	Prefer Forward Security		
	Pre-shared Key		

Configuring IPSec VPN in the Branch Office



Item	Function		Description
1	Connection Name	VPN_IPSec1	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.0.0	Branch office network (refer to Table 3)
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.1.121.3	IP address of the head office router (in WAN side)
4	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network (refer to Table 3)
	Netmask	255.255.255.0	
5	Authentication		Security plan (refer to Table 3)
	Encryption		
	Prefer Forward Security		
	Pre-shared Key		

QoS (Quality of Service)

QoS function helps you to control your network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream.

You can find two items under the **QoS** section: **Prioritization** and **IP Throttling** (bandwidth management).

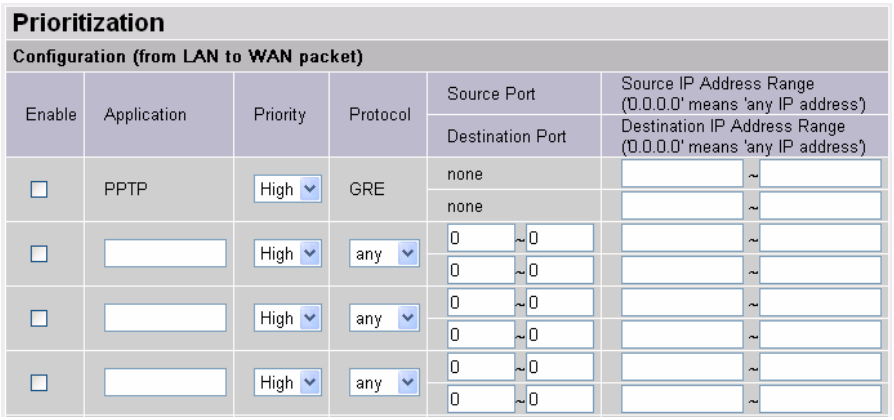
Prioritization

There are three priority settings to be provided in the modem:

- **High**
- **Normal** (The default is normal priority for all of traffic without setting).
- **Low**

The trigger of check can base on IP protocol, port number and address.

And the balance of utilization of each priorities are High(60%), Normal(30%) and Low(10%).



Prioritization

Configuration (from LAN to WAN packet)

Enable	Application	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means 'any IP address') / Destination IP Address Range ('0.0.0.0' means 'any IP address')
☐	PPTP	High	GRE	none	~
				none	~
☐		High	any	0 ~ 0	~
				0 ~ 0	~
☐		High	any	0 ~ 0	~
				0 ~ 0	~
☐		High	any	0 ~ 0	~
				0 ~ 0	~

Enable: Select it to activate the function.

Application: A name that identifies an existing rule.

Priority: High or Low, the priority for existing rule. All of traffic will be set to normal priority until you change it. The balance of utilizations for each priority is High (60%), Normal (30%) or Low (10%).

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

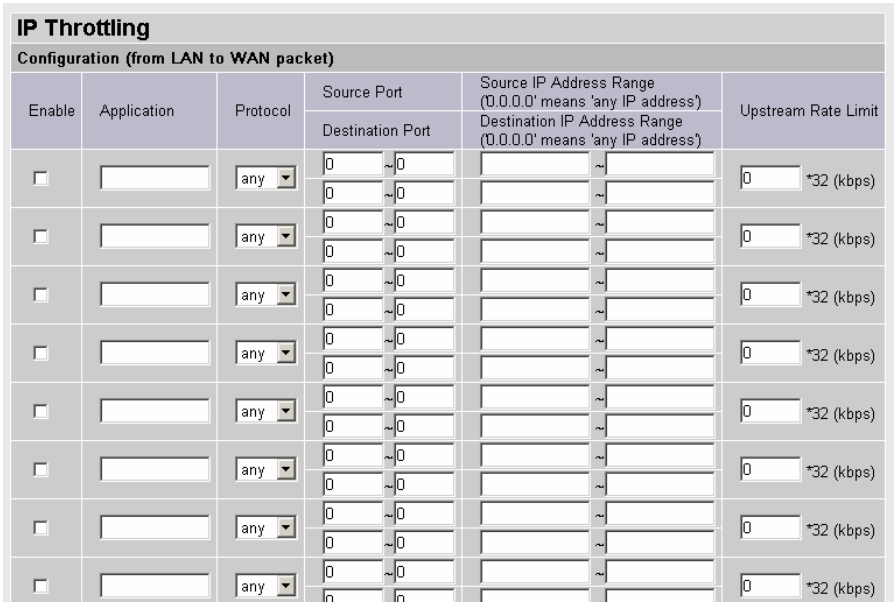
Source IP Address Range: The source IP address or IP range of packets to be monitored.

Destination IP address Range: The destination IP address or IP range of packets to be monitored.

IP Throttling

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.

The trigger of check can base on IP protocol, port number and address as well.



Enable: Select it to activate the function.

Application: A name that identifies an existing rule.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

Source IP Address Range: The source IP address or IP range of packets to be monitored.

Destination IP address Range: The destination IP address or IP range of packets to be monitored.

Upstream Rate Limit: This function allows you to limit the speed of IP traffic from LAN to WAN. The value entered will limit the speed of the application that you identified. The speed can be specified in multiple of 32kbps.

Virtual Server ("Port Forwarding")

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as "well-known ports". The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown in Table 4, for further information, please see IANA's website at:

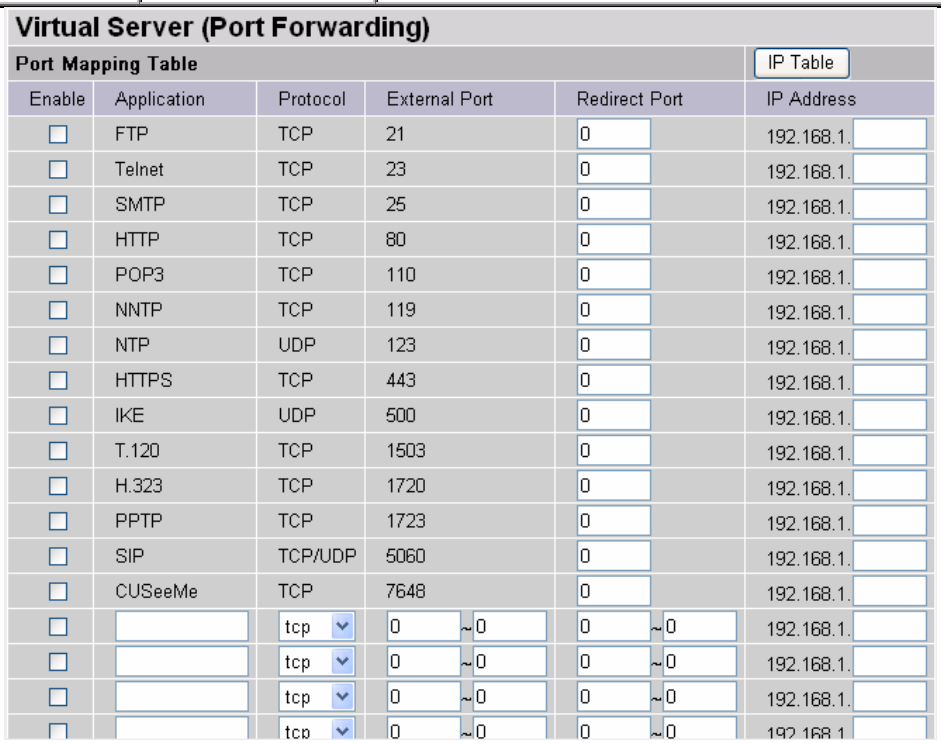
http://www.iana.org/assignments/port-numbers

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at: http://www.TeleWell.com

Table 4: Well-know and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP

110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio


Virtual Server (Port Forwarding)
Port Mapping Table
IP Table
Enable
Application
Protocol
External Port
Redirect Port
IP Address
FTP TCP 21 0 192.168.1.
Telnet TCP 23 0 192.168.1.
SMTP TCP 25 0 192.168.1.
HTTP TCP 80 0 192.168.1.
POP3 TCP 110 0 192.168.1.
NNTP TCP 119 0 192.168.1.
NTP UDP 123 0 192.168.1.
HTTPS TCP 443 0 192.168.1.
IKE UDP 500 0 192.168.1.
T.120 TCP 1503 0 192.168.1.
H.323 TCP 1720 0 192.168.1.
PPTP TCP 1723 0 192.168.1.
SIP TCP/UDP 5060 0 192.168.1.
CUSeeMe TCP 7648 0 192.168.1.
tcp 0 ~ 0 0 ~ 0 192.168.1.
tcp 0 ~ 0 0 ~ 0 192.168.1.
tcp 0 ~ 0 0 ~ 0 192.168.1.
tcp 0 ~ 0 0 ~ 0 192.168.1.

Because NAT can act as a "natural" Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users will be forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most

applications will use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to "all" will cause all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ: The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet received does not use a port number used by any other Virtual Server entries.

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or create a Virtual Server entry for "All" protocols, as doing so will result in all connection attempts to your public IP address will access the PC specified.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

Attention

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

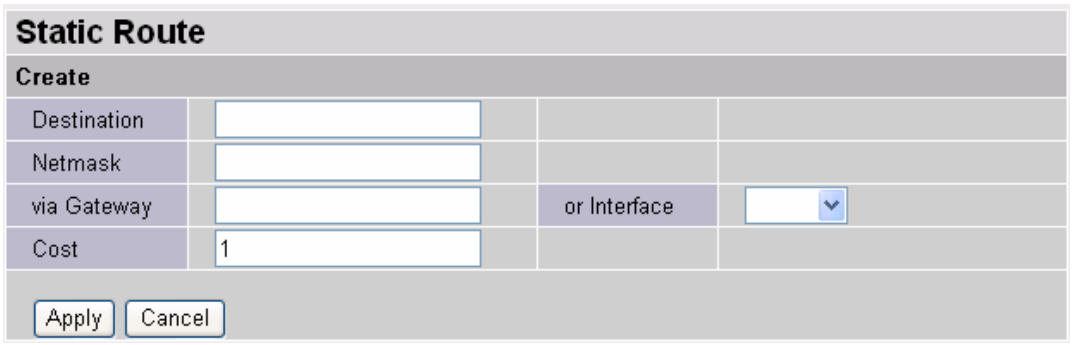
Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are four items within the **Advanced** section: **Static Route, Dynamic DNS**, **Checking Email** and **Device Management.**

Static Routing

Click on **Routing Table** and then choose **Create Route** add a routing table.



Destination: This is the destination subnet IP address.

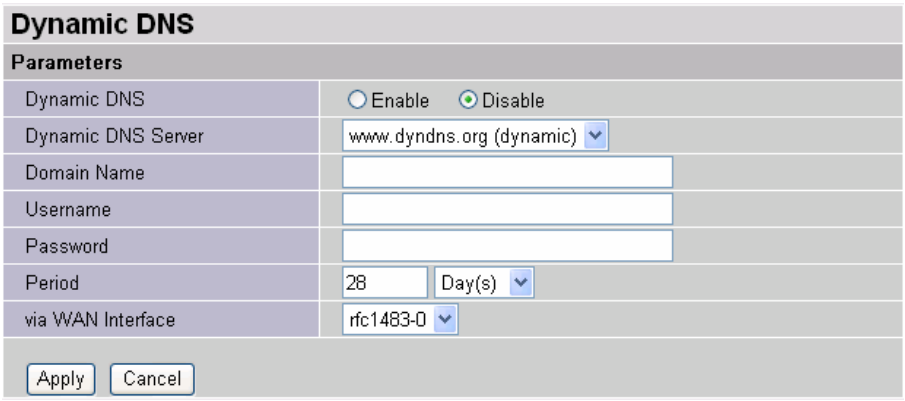
Netmask: Subnet mask of the destination IP addresses based on above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

Dynamic DNS



The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/

There are more than 5 DDNS services supported.

⊙ **Disable:** Check to disable the Dynamic DNS function.

⊙ **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required:

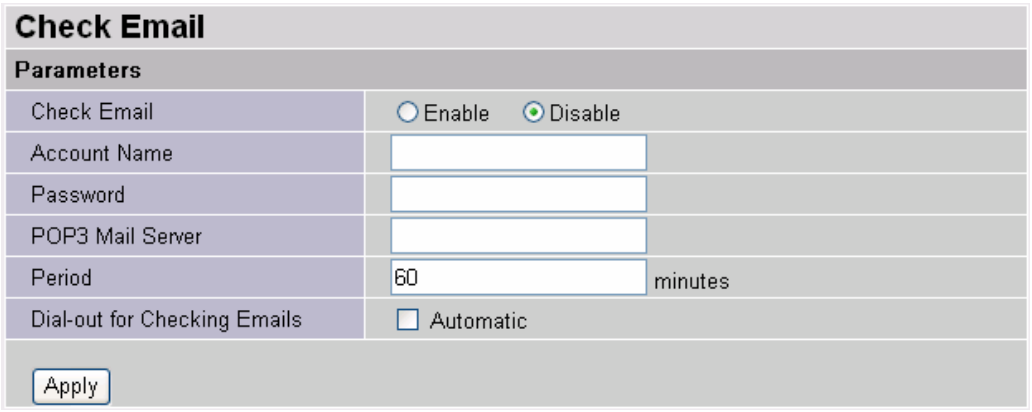
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Via WAN Interface: Decide which WAN interface you want to use for sending DDNS request.

Check Emails



This function allows you to have the router check your POP3 mailbox for new Email messages. The **Mail** LED on your router will light when it detects new messages waiting for download. You may also view the status of this function using the **Status – Email Checking** section of the web interface, which also provides details on the number of new messages waiting. See the **Status** section of this manual for more information.

⊙ **Disable:** Check to disable the router's Email checking function.

⊙ **Enable:** Check to enable the routers Emailing checking function. The following fields will be activated and required:

Account Name: Enter the name (login) of the POP3 account you wish to check.. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

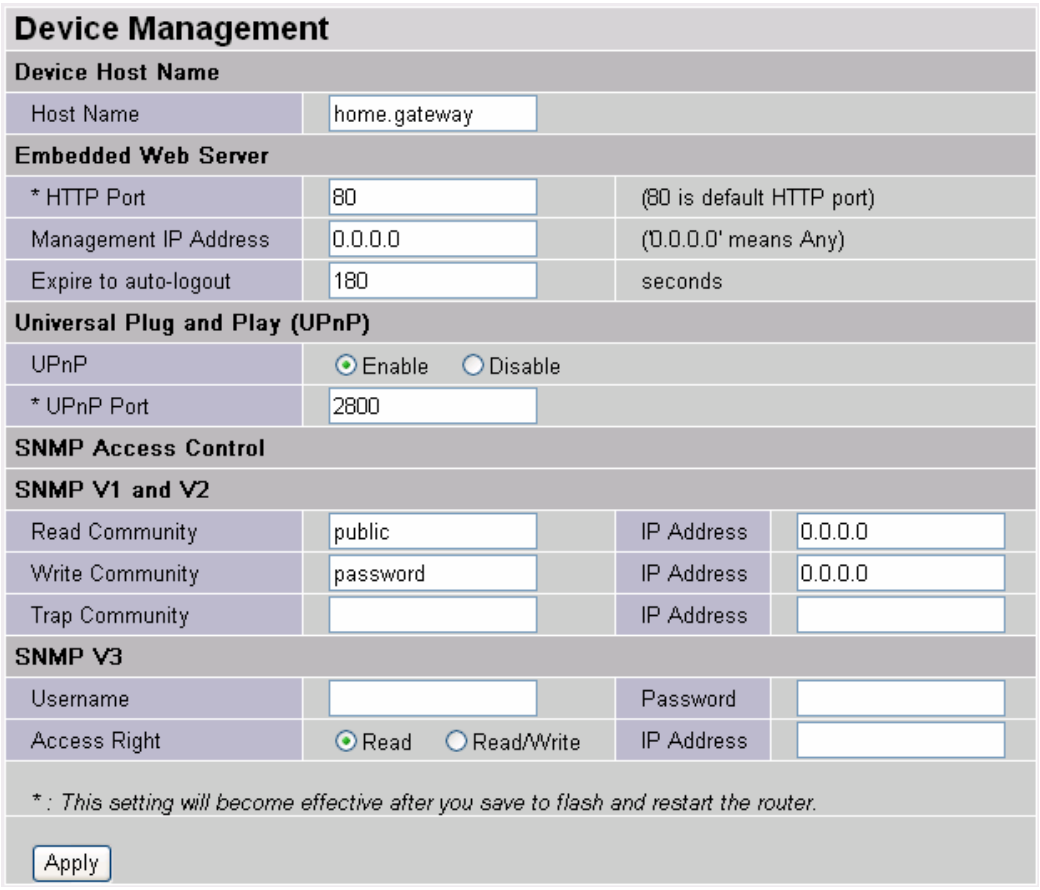
POP3 Mail Server: Enter your (POP) mail server name. You Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Interval: Enter the value in minutes between periodic mail checks.

Automatically dial-out for checking emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time online.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Embedded Web Server:

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.0.55**, and sets the logout time to be **100** seconds. The router will only allow User A access from the IP address **192.168.0.55** to logon to the Web GUI by typing: http://**192.168.0.254:100** in their web browser. After 100 seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

⊙ **Disable:** Check to disable the router's UPnP functionality.

⊙ **Enable:** Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

- **From RFC 1213 (MIB-II):**
  - ☑ System group
  - ☑ Interfaces group
  - ☑ Address Translation group
  - ☑ IP group
  - ☑ ICMP group
  - ☑ TCP group
  - ☑ UDP group
  - ☒ EGP (not applicable)
  - ☑ Transmission
  - ☑ SNMP group

- **From RFC1650 (EtherLike-MIB):**
  - ☑ dot3Stats

- **From RFC 1493 (Bridge MIB):**
  - ☑ dot1dBase group
  - ☑ dot1dTp group
  - ☑ dot1dStp group (if configured as spanning tree)

- **From RFC 1471 (PPP/LCP MIB):**
  - ☑ pppLink group
  - ☒ pppLqr group

- **From RFC 1472 (PPP/Security MIB):**
  - ☑ PPP Security Group)

- **From RFC 1473 (PPP/IP MIB):**
  - ☑ PPP IP Group

- **From RFC 1474 (PPP/Bridge MIB):**
  - ☑ PPP Bridge Group

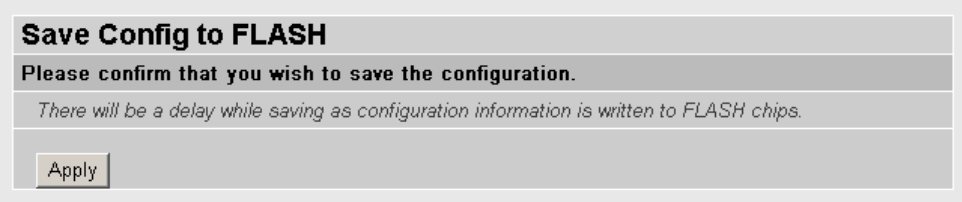
- **From RFC1573 (IfMIB):**
  - ☑ ifMIBObjects Group

- **From RFC1695 (atmMIB):**
  - ☑ atmMIBObjects

- **From RFC 1907 (SNMPv2):**
  - ☑ only snmpSetSerialNo OID

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them being lost after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.


Save Config to FLASH
Please confirm that you wish to save the configuration.
There will be a delay while saving as configuration information is written to FLASH chips.
Apply

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting your service provider or TeleWell support.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection ("linesync") failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problems, you may need to verify these settings with your ISP.

Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your TeleWell router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.

APPENDIX A: Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section of this manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

For further assistances with the product, please feel free to contact and visit us at: **http://www.TeleWell.com**

Mac OS is a registered Trademark of Apple Computer, Inc.
Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered Trademarks of Microsoft Corporation.

Declaration of Conformity

Manufacturer's Name: *Easytel oy*

Manufacturer's Address: *Alhotie 14 b 16*
04430 Järvenpää

declares that the product

Model Name: Telewell TW-EA2000 ADSL modem

Type of Product:

conforms to the following Product Specifications:

Safety: *EN60950 (1992) + A1 (1993) + A2 (1993) + A3 (1995) + A4 (1997) + A11 (199*

EMC: *EN 55022 (1998) Class B*
EN 55024 (1998)
EN 61000-3-2 (1995)
EN 61000-3-3 (1995)

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EE the EMC Directive 89/336/EEC, and the R&TTE Directive 1999/5/EC (Annex II) and carries CE-marking accordingly.

JARVENPAA, FINLAND 27.01.2004

Markku Åberg
General Manager